Rutin för behörighetshantering i socialförvaltningens verksamhetssystem

Diarienummer:	2022/00337
Paragraf:	§ -
Beslutsinstans:	Socialnämnden
Beslutsdatum:	2024-11-29
Informationsklassning:	K1, R1, T1, S2
Dokumentansvarig:	Förvaltningschef
Giltighetstid:	Beslutsdatum tills vidare
Föregående diarienummer:	
Föregående beslutsdatum:	
Föregående beslutsinstans:	
Föregående paragraf:	

Motala kommun
Socialförvaltningen

Motala kommun

Rutin för behörighetshantering i socialförvaltningens verksamhetssystem

Inledning

Behörigheter till socialförvaltningens/kommunens verksamhetssystem som innehåller känsliga personuppgifter regleras i olika författningar såsom dataskyddsförordningen, GDPR, patientdatalagen (2008:355) och lagen (2001:454) om behandling av personuppgifter inom socialtjänsten, SoLPuL. Personuppgifterna ska skyddas så att ingen obehörig kan få del av uppgifterna. Behörighetsstyrning och interna kontroller är en viktig del av arbetet med att skydda uppgifterna. I detta ligger att upprätta och upprätthålla rättigheter för användare i de IT-system som används så att användarna enbart får och har åtkomst till den information som behövs i det dagliga arbetet.

Personuppgiftsansvarig (socialnämnden) är skyldig att, i förhållande till riskerna, vidta lämpliga säkerhetsåtgärder (artikel 32 GDPR). Särskild hänsyn ska tas till de risker som behandlingen av personuppgifter medför, i synnerhet oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande av eller obehörig åtkomst till personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Syfte

Syftet med rutinen är att ge direktiv inför behörighetshantering så att bedömningarna sker enhetligt inom socialförvaltningen. Syftet är också att begränsa obehörigas åtkomst till uppgifter om enskilda samt att säkerställa att behörigheten inte är för snäv vilket kan medföra risker för den enskilde.

Rutin för behörighetshantering i socialförvaltningens verksamhetssystem

Villkor för behörighetstilldelning

Behörigheten ska begränsas till vad som behövs för att fullgöra arbetsuppgifter inom socialtjänsten. Detta gäller såväl tillsvidareanställd personal som personal med en tidsbegränsad anställning samt vissa studerande[1].

Enligt 10 § lagen (2001:454) om behandling av personuppgifter inom socialtjänsten ska den personuppgiftsansvarige för uppgifter om enskilda som förs helt eller delvis automatiserat

1. bestämma villkor för tilldelning av behörighet för åtkomst till sådana uppgifter,

[1] De studerande som får behörighet är endast studerande på socialkontoret (socionomer som får plats på utförare IFO) samt legitimerad personal. Således ej elever på gymnasienivå.

2. se till att åtkomst till sådana uppgifter dokumenteras och kan kontrolleras, och

3. göra systematiska och återkommande kontroller av om någon obehörigen kommer åt sådana uppgifter.

Behörigheten enligt första stycket 1 ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter inom socialtjänsten.

Enligt 4 kap. 2 § Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården ska vårdgivaren ansvara för att varje användare tilldelas en individuell behörighet för åtkomst till personuppgifter. Vårdgivarens beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys.

Personuppgiftsansvariges ansvar

- Behörighetstilldelning ska alltid föregås av en behovs- och riskanalys.

En alltför vidsträckt behörighet till personuppgifter innebär att personal kan få tillgång till fler uppgifter än de som behövs för att kunna utföra sitt arbete. Den enskildes upplevelse av att fler tar del av uppgifterna än vad som är nödvändigt för insatsernas utförande är viktig att beakta. Därför är det viktigt att endast de som behöver uppgifter om den enskilde för sina arbetsuppgifter har tillgång till dem.[2]

Behörighetstilldelning innebär att ansvarig ska göra aktiva och individuella behörighetstilldelningar utifrån analyser av vilken närmare information de olika personalkategorierna och olika verksamheter behöver.

Se även Integritetsskyddsmyndighetens information om behörighetsstyrning (referens).

Behovs- och riskanalys

Behörigheten ska motsvara det faktiska behovet och ska därmed varken vara för snäv vilket kan medföra säkerhetsrisker för patienter, brukare eller klienter eller för vid vilket kan innebära att den enskildes integritet påverkas negativt.

För att kunna bedriva en god och säker vård och omsorg krävs tillgång till relevant information. Vad som räknas som relevant baseras på verksamhetens uppdrag. En för vid/generös behörighet kan leda till konsekvenser som obefogad spridning av uppgifter eller förlorad riktighet i form av felaktig radering eller förändring av information. En för snäv behörighet kan innebära att användaren inte kan utföra sina arbetsuppgifter vilket kan medföra risker. Integritetsmyndigheten, IMY, har en vägledning för behovs- och riskanalys.

Följande risker ska beaktas;

- Risker som uppstår om medarbetare inom verksamheten eller enheten inte har tillgång till relevant information om den enskilde.

[2] Se prop. 2022/23:131 s. 45.

- Risker relaterade till en för bred/generös tillgång till information.

- Risker som kan påverka den enskildes fri- och rättigheter.

- Risker som leder till negativa konsekvenser för säkerheten eller att den enskildes integritet påverkas negativt.

Verksamhetschefens/enhetschefens ansvar

- Bedömning och beslut om behörighetstilldelning ska ske utifrån varje användares arbetsuppgifter.

- Behörighetstilldelning ska alltid tidsbegränsas vid visstidsanställningar.

- Användare ska informeras om de bestämmelser som gäller för hantering av uppgifter och om de regler och rutiner som gäller för respektive IT-stöd.

- Uppföljning av behörigheter ska ske fortlöpande och vid behov ska förändring av behörigheter ske (se rutin för loggkontroll i verksamhets-system och nationell patientöversikt, SN 2019/0335).

Utökad behörighet medarbetare

När det finns behov av undantag från de grundläggande principerna kan enhetschef i samråd med verksamhetschef och systemförvaltare fatta beslut om utökad behörighet. Utökad behörighet gäller tills man byter tjänst/behörighetsgrupp/roll eller avslutar ett uppdrag som behörigheten behövts för. Beslutet ska dokumenteras och motiveras.[3] Beslutet skickas i pappersform till systemförvaltare Viva.

Användarens ansvar

Varje användare ansvarar för att nedanstående följs:

- Tilldelad behörighet får inte delges annan användare.

- Lösenord får inte lämnas ut till annan person.

- Hjälpmedel för autentisering (till exempel SITHS-kort eller lösenordsdosa) får inte lånas ut till en annan användare.

- Användare ska alltid logga ut eller låsa IT-arbetsplatsen när den lämnas.

- Tilldelad behörighet får endast användas för att utföra tilldelad arbetsuppgift.

- Brister i rutiner eller andra oegentligheter ska rapporteras till närmaste chef.

Beställning av behörigheter m.m.

Behörig beställare

Behörig beställare är biträdande socialdirektör/förvaltningschef, verksamhetschef eller enhetschef.

För externa utförare är behörig beställare verksamhetschef/tf verksamhetschef. Denna person kan i sin tur utse personer som får beställa

[3] Se bilaga blankett.

behörighet för andra personer i företaget såsom gruppchef/planeringsledare.

Beställning av behörighet görs i Viva.

Beställning av behörigheter

Nya behörigheter eller ändrad behörighet utifrån förändrad anställning beställs i Inrule Process Automation, IPA (tidigare Barium).

Systemförvaltaren lägger upp användaren med behörighet enligt beställning i IPA.

Beställning av behörighet till hyrsjuksköterskor, studerande m.fl. görs i Topdesk. Beställning till IT-enheten.

För nyanställda eller vid förändrad anställning beställs behörighet i IPA (viktigt att detta görs vid förändrad anställning då behörigheter kan påverkas). Om ej ändrad anställning men om personal har resurstid görs ändringen i Topdesk eller av administratör/planerare på enheten. Vid ej ändrad anställning men behov av annan behörighet utifrån ändrat uppdrag ska ändringen beställas i Topdesk.

Det är möjligt att skapa utökad behörighet i vissa ärenden (i stället för att ge för bred behörighet i samtliga ärenden). Exempelvis mellan vuxengruppen och ekonomigruppen eller daglig verksamhet och boende LSS. Detta görs i samråd med någon av ansvariga chefer/verksamhetspedagog/1:e socialsekreterare/1:e behandlare och ska alltid journalföras med tydlig avsikt om orsak till att ärende delas.

För externa utförare beställs behörighet i Viva. Systemförvaltaren lägger upp användaren i Identity manager Dashboard för inlogg till datorn samt i Viva. Förändrad behörighet skickas i Viva. Efter varje avslutad månad ska extern utförare skicka in avslutad personal i Viva.

Uppföljning av användare

Vad gäller logguppföljning extern utförare som använder anmodat verksamhetssystem skickar verksamhetschef meddelande i Viva om vilka brukare/anställda som vi ska ta ut loggrapport på enligt extern utförares rutin om loggkontroll.

I övrigt - se Rutin för loggkontroll i verksamhetssystem och nationell patientöversikt, SN 2019/0335.

Bilagor

1 Blankett för dokumentation av utökade behörigheter

Referenser

GDPR

4 kap. 2 § och 6 kap. 7 § patientdatalagen (2008:355)

4 kap. 2 § Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården

Lagen (2001:454) om behandling av personuppgifter inom socialtjänsten, SoLPuL

Socialstyrelsens meddelandeblad 1/2024 Nya bestämmelser om behörighetstilldelning och kontroll av åtkomst till uppgifter för verksamheter inom socialtjänst och LSS

Välfärdsteknik inom äldreomsorgen, prop. 2022/23:131 s. 45

Se Integritetsmyndighetens information om behörighetsstyrning samt behovs- och riskanalys – www.imy.se