Meddelandeblad

Nr 1/2024

Mottagare: Kommuner, regioner, Statens institutionsstyrelse, juridiska och fysiska personer som ansvarar för privat verksamhet utifrån socialtjänstlagen och LSS

Nya bestämmelser om behörighetstilldelning och kontroll av åtkomst till uppgifter för verksamheter inom socialtjänst och LSS

Den 1 mars 2024 träder bestämmelser om behörighetstilldelning och åtkomstkontroll i kraft i lagen (2001:454) om behandling av personuppgifter inom socialtjänsten, SoLPUL. De gäller för hela socialtjänsten och all verksamhet som bedrivs med stöd av LSS. Regleringen avser tillgång till uppgifter om enskilda personer som förs helt eller delvis automatiserat. Bestämmelserna syftar till att begränsa obehörigas åtkomst till uppgifter om enskilda.[1]

I korthet handlar bestämmelserna om att personuppgiftsansvariga ska göra följande:

- bestämma villkor för tilldelning av åtkomst till uppgifter som förs helt eller delvis automatiserat,
- skapa förutsättningar för kontroll av åtkomst till sådana uppgifter och
- kontrollera obehörig åtkomst systematiserat och återkommande.

[1] Se prop. 2022/23:131 s. 59.

Socialstyrelsen

För vem gäller bestämmelserna?

Reglerna ska tillämpas av den som är personuppgiftsansvarig. För en kommunal verksamhet är den kommunala myndigheten personuppgiftsansvarig.[2] För privat verksamhet[3] är det den juridiska eller fysiska person som ansvarar för verksamheten som är personuppgiftsansvarig.[4]

Bestäm villkor för tilldelning av behörighet

Den personuppgiftsansvarige ska bestämma villkor för tilldelning av behörighet som avser åtkomst till uppgifter om enskilda som förs helt eller delvis automatiserat.[5]

Med åtkomst avses tillgång till uppgifter som behandlas inom den egna organisationen. Bestämmelserna om behörighetstilldelning innebär att den verksamhetsansvarige ska göra aktiva och individuella behörighetstilldelningar utifrån analyser av vilken närmare information olika personalkategorier och olika slags verksamheter behöver. När villkoren för behörighetstilldelning bestäms måste också riskanalyser göras. Vid utformning av behörighetssystem måste de grundläggande principerna för behandling av personuppgifter i artikel 5 i EU:s dataskyddsförordning[6] beaktas.[7] De grundläggande principerna är laglighet, korrekthet och öppenhet, ändamålsbegränsning, uppgiftsminimering, riktighet, lagringsminimering, integritet och konfidentialitet.[8]

I system som många har behörighet till ska normalt olika behörighetsnivåer för personalen finnas. Mer känsliga uppgifter får inte vara lika enkelt åtkomliga för personalen som mindre känslig information. Det ingår i ansvaret för den som bedriver socialtjänst att se till att alla anställda får full information om behörighetsreglerna. Behörighetstilldelningen bör åtföljas av tekniska begränsningar, så att den som inte har behörighet att ha tillgång till vissa uppgifter inte heller har teknisk möjlighet att komma åt dessa. Behörigheter måste också följas upp och ändras efter hand som ändringar i personalens arbetsuppgifter ger anledning till det.[9]

---

[2] 11 § förordningen (2001:637) om personuppgiftsbehandling inom socialtjänsten, SoLPUF.
[3] Att socialtjänst i det här sammanhanget även omfattar verksamhet enligt lagstiftningen om stöd och service till vissa funktionshindrade framgår av 2 § första stycket 5 SoLPUL.
[4] 17 § SoLPUF.
[5] Se 10 § första stycket 1 SoLPUL.
[6] Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[7] Prop. 2022/23:131 s. 59.
[8] Mer information finns på Integritetsskyddsmyndighetens webbplats, www.imy.se.
[9] Prop. 2022/23:131 s. 59.

Ansvaret vid tilldelning av behörighet för elektronisk åtkomst innefattar en skyldighet att göra aktiva och individuella behörighetstilldelningar utifrån analyser av vilken information olika personalkategorier och olika slags verksamheter behöver (behovsanalys). Användarna behöver tilldelas rätt behörighet, dvs. tillräcklig behörighet, för att kunna utföra sina arbetsuppgifter på ett säkert sätt utan att behörigheten blir mer omfattande än vad som är nödvändigt. Den personuppgiftsansvarige måste också se till att det finns rutiner för att ändra, ta bort och regelbundet följa upp behörigheter.[10]

Begränsa behörigheten

Behörigheten ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter inom socialtjänsten.[11] Uttrycket var och en inkluderar såväl tillsvidareanställd personal som t.ex. personer med en tidsbegränsad anställning. Att begränsa behörigheten efter behov kan handla om att begränsa en enskild medarbetares möjlighet att ta del av personuppgifter utifrån vad som behövs vid arbete med exempelvis ärendehantering, utförande av insatser inom socialtjänsten eller dokumentation av sådana insatser.[12]

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 inom socialtjänsten. Konsekvenser av att uppgifter hamnar fel och hur allvarligt det är beror på uppgifternas art, vem det rör och andra omständigheter. Den enskildes upplevelse av att fler tar del av uppgifterna än vad som är nödvändigt för insatsernas utförande är också viktig att beakta. Det är därför viktigt att endast de som behöver uppgifter om den enskilde för sina arbetsuppgifter har tillgång till dem.[13]

Skapa förutsättningar för kontroll av åtkomst

Utöver att bestämma villkor för tilldelning av behörighet till uppgifter som förs helt eller delvis automatiserat ska personuppgiftsansvariga också se till att åtkomst till sådana uppgifter dokumenteras och kan kontrolleras.[14]

Den personuppgiftsansvarige är skyldig att se till att all åtkomst till uppgifter om enskilda dokumenteras och kan kontrolleras. Det gäller både den egna personalens åtkomst och den åtkomst som bereds andra. Om det är möjligt att få åtkomst till personuppgifter som behandlas helt eller delvis

[10] Prop. 2022/23:131 s. 45.
[11] 10 § andra stycket SoLPUL.
[12] Se prop. 2022/23:131 s. 60.
[13] Se prop. 2022/23:131 s. 45.
[14] Se 10 § första stycket 2 SoLPUL.

automatiserat via öppna nät som internet eller molntjänst behöver identiteten av den som bereder sig åtkomst säkerställas. Det kan ske genom exempelvis stark autentisering[15].[16] Krav på autentisering framgår indirekt av kraven i artikel 32 i EU:s dataskyddsförordning.[17]

Åtkomstkontroller ska göras för att bland annat kunna säkerställa att användare inte använder sina behörigheter på fel sätt genom att läsa, ändra eller ta bort uppgifter som de inte ska behandla. Exempel på en felaktig åtkomst kan vara att någon öppnar den enskildes dokumentation trots att hen inte har med den enskilde att göra. För att den som bedriver socialtjänst ska kunna kontrollera att behörigheterna används på ett korrekt sätt måste åtkomsten till personuppgifter dokumenteras (loggas). Av loggarna ska användarens identitet framgå och vid vilken tidpunkt som åtkomsten skett. Loggarna måste sparas en tid för att möjliggöra kontroll.[18]

Genomför systematiska och återkommande åtkomstkontroller

Den personuppgiftsansvarige blir även skyldig att göra systematiska och återkommande kontroller av om någon obehörigen kommer åt uppgifter om enskilda som förs helt eller delvis automatiserat.[19]

Hur regelbundna kontrollerna ska vara måste bedömas utifrån verksamhetens omfattning, antalet personer med åtkomst, modellen för behörighetstilldelning och kontrollens omfattning. Kontrollen bör vara baserad på en riskanalys som den personuppgiftsansvarige genomför.[20]

Systematiska och återkommande stickprovskontroller av loggarna behöver göras och antalet stickprovskontroller ska vara proportionerliga i förhållande till antalet slagningar som görs i systemet. Det räcker inte att bara göra uppföljningskontroller i särskilda fall då misstanke kan finnas om obehörigt intrång. Uppgiftskontroller ska göras systematiskt och fortlöpande oberoende av misstanke.[21]

[15] Stark autentisering kan beskrivas som ett samlingsnamn för tekniska funktioner som säkerställer en användares identitet genom användarcertifikat, engångslösenord eller motsvarande, det vill säga en högre grad av verifiering av en uppgiven identitet än enbart användarnamn och lösenord.
[16] Prop. 2022/23:131 s. 59.
[17] Se prop. 2022/23:131 s. 45.
[18] Se prop. 2022/23:131 s. 59 f.
[19] Se 10 § första stycket 3 SoLPUL.
[20] Prop. 2022/23:131 s. 46.
[21] Prop. 2022/23:131 s. 60.

Denna information (artikelnr 2024-1-8917) kan laddas ner från socialstyrelsen.se/publikationer.