Uppföljning av intern kontrollplan 2026

Grundskolenämnden

Malmö stad

Innehållsförteckning

Inledning 3

Granskningar.....4

Nämndens granskningar 4

Risk: Risk för felaktig hantering av personuppgifter 4

Granskning: Granskning av hantering av personuppgifter.....4

Inledning

Den interna kontrollen ingår i grundskolenämndens samlade styr- och ledningssystem. Grundskolenämnden har det yttersta ansvaret för att den interna kontrollen är tillräcklig samt att verksamheten bedrivs på ett tillfredsställande sätt. Den interna kontrollen ska vara praktiskt och ändamålsenligt uppbyggd utifrån verksamhetens behov och förutsättningar samt hantera risker och förebygga att fel uppstår genom att vara ett verktyg för att se till att:

- verksamheten är ändamålsenlig och effektiv
- information om verksamhet och ekonomi är tillförlitlig
- lagar, förordningar och styrdokument efterlevs
- säkra tillgångar och förhindra förluster samt upptäcka och eliminera eller förebygga allvarliga fel.

I grundskolenämndens interna kontrollplan för 2026 anges vilka olika granskningsområden som ska följas upp under året. Granskningarna återrapporteras till nämnden löpande under året i separata rapporter liksom denna.

Granskningar

Nämndens granskningar

Risk: Risk för felaktig hantering av personuppgifter

Beskrivning av risk

Det finns en otydlighet i hur personuppgifter för personal med skyddad identitet hanteras i olika system samt hur man ska kunna lösa exempelvis myndighetsutövning, fakturering och utbetalning av lön utan att röja deras identitet.

Enhet

Avdelning stöd och utveckling

Granskning: Granskning av hantering av personuppgifter

Områden och tillhörande rutiner som ska granskas:

System som hanterar skyddade personuppgifter

Syfte med granskningen:

Inventera vilka system som utbyter data. Identifiera kritiska överföringspunkter där skyddet riskerar att falla bort.

Omfattning/avgränsning:

Denna kartläggning omfattar de system som förvaltas av grundskoleförvaltningen eller sektionen för systemförvaltningen alternativt system med manuell behörighetshantering där behörigheterna hanteras av medarbetare i grundskoleförvaltningen (inte centralt).

Stadskontoret jobbar på en stadsgemensam rutin för hantering av skyddade personuppgifter där vi väntar in resultaten, men hoppas att den innefattar de system som driftas centralt. ITD på serviceförvaltningen har även gjort en utredning av flödet av personuppgifter mellan Personec P och Active Directory som skickar vidare information till en del av våra system.

Granskningsmetod:

Systemkartläggning: Inventera vilka system som utbyter data. Identifiera kritiska överföringspunkter där skyddet riskerar att falla bort.

Observation: Sitt med en handläggare och följ ett ärende "live" i systemet. Kontrollera visuellt om skyddade personuppgifter syns i rullgardinsmenyer, sökfält eller på utskrifter/fakturaunderlag.

Intervjuer: Fokusera på de manuella rutinerna. Fråga hur personalen praktiskt löser myndighetsutövning eller utbetalningar när systemet spärrar.

Klargöra hur processen fungerar för personal som får skydd i relation till de delar av processen som hanteras av ITD på serviceförvaltningen.

Behörighetskontroll: Begär ut loggar på vilka som har läsrättigheter till skyddade personuppgifter. Kontrollera om kretsen är strikt begränsad.

Analys: Bedöm om riskerna är tekniska (systemet klarar inte av att maska uppgifter) eller organisatoriska (fel handhavande/för breda behörigheter).

Resultat

Kategorier av system

Kartläggningen har mynnat ut i tre kategorier av system, som innehar sina egna utmaningar.

1. System med manuell behörighetshantering utan integration för persondata

Den första kategorin omfattar system där användarkonton och behörigheter administreras manuellt och där det saknas automatiska integrationer mot stadens centrala identitets- och behörighetshantering. Dessa system tar inte emot användaruppgifter från exempelvis AD, Personec P eller Edlevo, vilket innebär att konton och behörigheter skapas och underhålls lokalt av systemadministratörer eller verksamheten.

Trots att systemen saknar automatiserade personflöden innehåller många av dem fortfarande personuppgifter. Eftersom administrationen sker manuellt finns det normalt ingen mekanism som informerar systemägare eller behörighetsadministratörer om en person har skyddade personuppgifter eller om ett skydd tillkommer efter att användaren redan har lagts upp i systemet. Risken är därför att personuppgifter lagras, visas eller används på ett sätt som inte är anpassat för personer med skyddad identitet.

En ytterligare utmaning är att dessa system i regel inte använder fiktiva identiteter eller alternativa konton. Användarna registreras därför med sina faktiska personuppgifter, vilket innebär att skyddade personuppgifter förekommer direkt i systemen om ingen särskild manuell hantering genomförs. För system som använder inloggning via Freja eID behöver användaren dessutom identifiera sig med de verkliga personuppgifter som är kopplade till den personliga e-tjänstelegitimationen. Detta begränsar möjligheterna att använda alternativa identiteter eller fiktiva personnummer för att skydda användarens identitet.

Den främsta risken inom denna kategori är därför inte spridning via integrationer, utan avsaknaden av information om skyddsstatus och beroendet av manuella rutiner. Om verksamheten saknar kännedom om att en användare har eller har fått skyddade personuppgifter finns en risk att

uppgifter registreras, exponeras eller hanteras på samma sätt som för övriga användare. Hanteringen blir därmed starkt beroende av att lokala administratörer känner till skyddet och löpande uppdaterar informationen i respektive system.

2. System med överföring från AD, Azure Entra ID eller Personec P

Den andra kategorin omfattar system som är anslutna till Malmö stads centrala identitets- och integrationsplattformar. För dessa system sker hanteringen av användaridentiteter genom ett sammanhängande informationsflöde där personuppgifter först registreras i Personec P, som utgör den primära källan för anställningsinformation. Det är också i Personec P som uppgifter om skyddade personuppgifter registreras och hanteras.

När en anställd har skyddade personuppgifter kan den ordinarie automatiserade identitetshanteringen inte användas fullt ut. I stället skapas ett manuellt användarkonto i Active Directory (AD), baserat på en alternativ identitet. Detta konto fungerar därefter som den identitet som används i den fortsatta digitala miljön.

Från AD synkroniseras användaren vidare till bland annat Azure Entra ID (Microsoft 365) och Metakatalogen och därifrån till andra system som använder central inloggning och behörighetshantering. Samtidigt överförs identitetsinformationen via stadens metakatalog till ett stort antal verksamhetssystem och digitala tjänster. På så sätt fungerar AD och Metakatalogen som nav i den fortsatta spridningen av användaridentiteten mellan olika system.

Förenklat kan flödet beskrivas enligt nedan:

Personec P → Manuell skyddad identitet i AD → Metakatalog → Verksamhetssystem/tjänster

Det är inom denna kategori som de mest komplexa utmaningarna kring skyddade personuppgifter har identifierats.

När en medarbetare får skyddade personuppgifter behöver verksamheten ta ställning till hur personens digitala identitet ska hanteras. I den nuvarande processen behöver medarbetare och chef, med stöd av ansvariga funktioner, välja om personen ska fortsätta använda sitt verkliga namn och personnummer eller om en helt eller delvis fiktiv identitet ska användas i de centrala identitetssystemen. De uppgifter som registreras i AD, blir därefter källan för ett stort antal anslutna system. Valet påverkar därför inte bara ett enskilt system utan hela den digitala identiteten och de integrationer som är kopplade till den.

En central utmaning är att det kan vara svårt för både chefer och medarbetare att förstå innebörden av de olika alternativen. Att behålla verkligt namn eller personnummer kan underlätta vissa funktioner och administrativa processer, men innebär samtidigt att personuppgifter kan bli synliga i fler system. Att använda fiktiva uppgifter kan ge ett starkare skydd,

men kan samtidigt påverka inloggning, behörighetsstyrning, sökbarhet, användarupplevelse och integrationer mellan system. Konsekvenserna varierar dessutom mellan olika verksamhetssystem, vilket gör det svårt för verksamheten att förutse effekterna av de val som görs.

Eftersom de uppgifter som registreras i de centrala katalogtjänsterna sprids vidare till många mottagande system kan ett beslut som fattas tidigt i processen få omfattande följdeffekter. Det skapar ett behov av tydligare vägledning, bättre beslutsstöd och en mer standardiserad hantering så att chefer och medarbetare inte själva behöver bedöma de tekniska och verksamhetsmässiga konsekvenserna av olika identitetslösningar.

Ur ett riskperspektiv innebär dagens hantering att skyddsnivån inte enbart avgörs av tekniska lösningar utan också av hur väl de inblandade personerna förstår processen och dess konsekvenser. Detta skapar en risk för oenhetlig hantering mellan olika verksamheter och för att val görs utan full förståelse för hur information kommer att visas, användas och spridas i de anslutna systemen.

3. System med överföring från Edlevo

Den tredje kategorin omfattar system som får användaruppgifter från Edlevo eller från elev- och personaldata som passerar genom Edlevo innan de distribueras vidare till andra system. För dessa system finns sedan tidigare etablerade rutiner för hantering av skyddade personuppgifter. Grundprincipen är att personer med skyddade personuppgifter inte förs vidare från Edlevo till anslutna system genom de ordinarie integrationsflödena.

Denna modell minskar risken för att skyddade uppgifter sprids vidare till ett stort antal mottagande system och innebär att skyddsbehovet hanteras redan vid källan. Konsekvensen är samtidigt att vissa system saknar automatisk information om dessa användare, vilket kan kräva separata administrativa rutiner för tilldelning av konton, behörigheter eller åtkomst till tjänster i de fall som skyddade personer behöver åtkomst till kringsystemen. Därmed flyttas utmaningen från informationsspridning till verksamhetens manuella hantering av användare och behörigheter.

Ur ett informationssäkerhetsperspektiv innebär denna lösning att integrationskedjan blir enklare att kontrollera eftersom den skyddade individens uppgifter stoppas innan de når efterföljande system. Samtidigt krävs tydliga och dokumenterade rutiner för att säkerställa att användarna kan utföra sina arbetsuppgifter utan att skyddet äventyras och utan att verksamheten blir alltför beroende av manuella arbetsmoment.

Analys
Utifrån genomförd kartläggning bedöms behovet av gemensamma och tydligt dokumenterade processer vara den viktigaste framgångsfaktorn för en säker hantering av skyddade personuppgifter.

Centrala processer och ansvar

Grundskoleförvaltningen ser ett behov av stadsgemensamma rutiner, ansvarsfördelningar och dokumenterade informationsflöden etableras för de system och identitetsplattformar som hanteras centralt. Det är särskilt viktigt att det finns tydlig dokumentation över hur skyddade personuppgifter hanteras i flöden mellan Personec P, AD, Azure Entra ID, Metakatalogen och anslutna verksamhetssystem. Detta minskar beroendet av enskilda personer och skapar bättre förutsättningar för en likvärdig hantering i hela staden.

Tydligare beslutsstöd vid skapande av skyddade identiteter

För system i kategori 2 behöver chefer och medarbetare få ett tydligare beslutsstöd när en skyddad identitet ska skapas. Det behöver framgå vilka konsekvenser olika val får ur såväl säkerhets- som verksamhetsperspektiv, exempelvis när verkliga respektive fiktiva personuppgifter används. Målet bör vara att den enskilda chefen inte själv ska behöva bedöma tekniska konsekvenser och risker i stadens identitets- och integrationsmiljö. Detta hanteras centralt i staden och håller på att ses över av stadskontoret. Förvaltningen följer därför det arbetet och avvaktar om eventuella åtgärder behöver vidtas utifrån detta.

Rutiner för system med manuell behörighetshantering

För system i kategori 1 ser förvaltningen behov av att en särskild rutin tas fram för hur behörighetsansvariga informeras när en medarbetare har eller får skyddade personuppgifter. Rutinen bör beskriva:

- hur information om skyddsstatus kommuniceras,
- när användarkonton bör avslutas eller begränsas,
- hur personuppgifternas synlighet ska bedömas i respektive system,
- vilka alternativa lösningar som kan användas när åtkomst fortfarande behövs.

För de system där det är tekniskt möjligt bör även användning av alternativa eller fiktiva identiteter utredas som ett sätt att minska exponeringen av personuppgifter.

Gemensam hantering inom Edlevo-miljön

För system i kategori 3 finns det behov av att fortsatt arbete samordnas med införandet av aliasmodulen i Edlevo. I samband med detta ser förvaltningen stora fördelar med att en gemensam rutin tas fram för samtliga skolförvaltningar där ansvar, arbetssätt och hantering av skyddade personuppgifter beskrivs på ett enhetligt sätt. Detta hade skapat förutsättningar för en konsekvent hantering oavsett skolförvaltning och har påbörjats kopplat till Edlevos nya Aliasmodul.

Samverkan mellan skolförvaltningarna

Kartläggningen visar att skyddade personer ofta kan förekomma i flera roller samtidigt, exempelvis som medarbetare i en förvaltning, vårdnadshavare i en annan och elev inom ytterligare en verksamhet. För att minska risken för skillnader i hanteringen behöver grundskoleförvaltningen, gymnasie- och vuxenutbildningsförvaltningen samt förskoleförvaltningen ha gemensamma rutiner, gemensamma riskbedömningar och en samordnad informationshantering för personer med skyddade personuppgifter.

Samlad bedömning

Den största risken i nuläget är inte en enskild teknisk lösning utan att hanteringen varierar mellan system, verksamheter och ansvariga funktioner. En mer standardiserad och förvaltningsövergripande hantering bedöms därför vara den åtgärd som ger störst effekt både ur informationssäkerhets- och verksamhetsperspektiv. Förvaltningen kommer fortsätta att arbeta tillsammans med de övriga skolförvaltningarna för att gemensamt hantera de risker som identifierats.

Åtgärd	Vad ska göras:
Ta fram rutin för behörighetsansvariga	Ta fram en rutin för hur behörighetsansvariga informeras när en medarbetare har eller får skyddade personuppgifter. Rutinen bör beskriva: •hur information om skyddsstatus kommuniceras, •när användarkonton bör avslutas eller begränsas, •hur personuppgifternas synlighet ska bedömas i respektive system, •vilka alternativa lösningar som kan användas när åtkomst fortfarande behövs. För de system där det är tekniskt möjligt bör även användning av alternativa eller fiktiva identiteter utredas som ett sätt att minska exponeringen av personuppgifter.