

Socialnämnden

2020-10-20

Socialnämnden

Tid 2020-10-20, kl 18:00

Plats Munkhättevägen 49 eller via Teams

Ärenden

Justering

- 1 Våldspreventivt arbete - muntlig information
- 2 Snabbspår Botkyrka – muntlig information
- 3 Remissvar betänkande Kontroll för ökad tilltro - en ny myndighet för att förebygga, förhindra och upptäcka felaktiga utbetalningar från välfärdssystemet, SOU 2020:35, Fi2020/02668/BATOT (SN 2020:317)
- 4 Granskning av intrångsskydd och IT-säkerhet i verksamhetssystem - Botkyrka kommun 2020-rapport KS/2020:444 (SN 2020:384)
- 5 Förvaltningschefen informerar - muntlig information
- 6 Samordningsförbundet Botkyrka, Huddinge och Salem (SN 2020:25)
- 7 Anmälan av delegationsbeslut 2020 (SN 2020:12)
- 8 Anmälningsärenden 2020 (SN 2020:10)

Var vänlig och meddela Anneli Sjöberg om du inte kan närvara, tfn 0708-86 13 39 eller anneli.sjoberg@botkyrka.se.

NIKLAS GLADH
ordförande

ANNELI SJÖBERG
sekreterare



1

Socialförvaltningens våldspreventiva arbete - muntlig information

Beslut

Socialnämnden har tagit del av informationen.

Ärendet

IFO-chef Gunilla Berghager informerade om det våldspreventiva arbetet.



2

Snabbspår Botkyrka - muntlig information

Beslut

Socialnämnden har tagit del av informationen.

Ärendet

IFO-chef Charlotte Lagerkvist, socialförvaltningen och verksamhetschef Kerstin Berglund, arbetsmarknads- och vuxenutbildningsförvaltningen informerade om Snabbspår Botkyrka, ett samarbete mellan socialförvaltningen och Arbetsmarknads- och Vuxenutbildningsförvaltningen.

**3****Remissvar betänkande Kontroll för ökad tilltro - en ny myndighet för att förebygga, förhindra och upptäcka felaktiga utbetalningar från välfärdssystemet, SOU 2020:35, Fi2020/02668/BATOT (SN 2020:317)****Beslut**

Socialnämnden godkänner förslag till yttrande och överlämnar det till Finansdepartementet.

Sammanfattning

Finansdepartementet har begärt remissvar från Botkyrka kommun. Kommunledningsförvaltningen har begärt att socialnämnden ska inkomma med ett remissvar. Botkyrka kommuns remissvar ska vara Finansdepartementet tillhanda senast den 30 oktober 2020.

Regeringen har givit en särskild utredare i uppdrag att undersöka hur en samordnad funktion för statliga utbetalningar från välfärdssystemet kan bidra till att öka möjligheterna att förhindra felaktiga utbetalningar, effektivisera utbetalningsprocesser och förbättra servicen till medborgare.

Utredningen föreslår att en särskild myndighet, Myndigheten för utbetalningskontroll, inrättas. Utredningen föreslår vidare att ett system med transaktionskonto, som hanterar utbetalningar från statliga välfärdsmyndigheter och Skatteverket, ska införas.



2020-09-14

Dnr SN/2020:317

Referens

Merith Fröberg, verksamhetsutvecklare

Mottagare

Socialnämnden
Kommunstyrelsen
Finansdepartementet**Remissvar av betänkandet Kontroll för ökad tilltro – en ny myndighet för att förebygga, förhindra och upptäcka felaktiga utbetalningar från välfärdssystemet, SOU 2020:35, Fi2020/02668/BATOT****Förslag till beslut**

Socialnämnden godkänner förslag till yttrande och överlämnar det till Finansdepartementet.

Sammanfattning

Finansdepartementet har begärt remissvar från Botkyrka kommun. Kommunledningsförvaltningen har begärt att socialnämnden ska inkomma med ett remissvar. Botkyrka kommuns remissvar ska vara Finansdepartementet tillhanda senast den 30 oktober 2020.

Ärendet

Regeringen har givit en särskild utredare i uppdrag att undersöka hur en samordnad funktion för statliga utbetalningar från välfärdssystemet kan bidra till att öka möjligheterna att förhindra felaktiga utbetalningar, effektivisera utbetalningsprocesser och förbättra servicen till medborgare.

Utredningen föreslår att en särskild myndighet, Myndigheten för utbetalningskontroll, inrättas. Utredningen föreslår vidare att ett system med transaktionskonto, som hanterar utbetalningar från statliga välfärdsmyndigheter och Skatteverket, ska införas.

Myndigheten för utbetalningskontroll ska ha i uppdrag att:

- administrera systemet med transaktionskonto,
- göra dataanalyser och urval i syfte att upptäcka och förhindra delaktiga utbetalningar från välfärdssystemet,
- genom inledande och fördjupande granskning hantera, sortera och analysera urvalsträffar, och

2018-08-27

Dnr SN/2018:328

- stödja och följa statliga myndigheter och arbetslöshetskassors arbete med att motverka felaktiga utbetalningar från välfärdssystemen.

Inrättandet ett system med transaktionskonto, som samlar utbetalningar från flera myndighet bedöms både effektivisera och ge en överblick över välfärdens utbetalningar som helhet. De utbetalningar som föreslås omfattas av den nya myndigheten är utbetalningar från Arbetsförmedlingen, Centrala Studiestödsnämnden, Försäkringskassan, Pensionsmyndigheten samt Skatteverket. I vissa delar ska även arbetslöshetskassorna omfattas.

Kommuner och regioner föreslås inte kunna ansluta sig till systemet i inledningsskedet. Utredningen föreslår dock att möjligheterna för kommuner och regioner att ansluta sig ska utredas vidare.

Myndigheten för utbetalningskontroll föreslås inleda sin verksamhet från och med 1 juli 2022.

Socialnämndens synpunkter på förslaget

Utredningens förslag ska förebygga, förhindra och upptäcka felaktiga utbetalningar från de statliga välfärdssystemen. Socialnämnden delar utredningens uppfattning att en särskild myndighet för utbetalningskontroll och ett system med transaktionskonto bör inrättas.

För att kunna motverka felaktiga utbetalningar behöver välfärdssystemet, enligt utredningen, ses som ett sammanhängande system, och att information om utbetalningar från välfärdssystemet samlas. Kommuner och regioner ska emellertid inte kunna ansluta sig, åtminstone inte initialt. Utredningen konstaterar emellertid att det inte finns anledning att anta att kommuner skulle vara mindre utsatta för bedrägerier än statliga myndigheter inom välfärdssystemen. Till exempel slår utredningen fast att hemtjänst och personlig assistans tillhör riskbranscherna för ekonomisk brottslighet. Att erbjuda hemtjänst är ett kommunalt uppdrag, liksom att tillhandahålla personlig assistans till personer som har behov av maximalt 20 timmar per vecka. Även ekonomiskt bistånd är ett område som utsätts för bedrägeri, och där vissa kommuner noterat en ökning av bedrägerier. Socialnämnden instämmer i slutsatsen att en särskild myndighet för utbetalningskontroll bör inrättas, men menar att även vissa utbetalningar från kommuner bör kunna omfattas.

Syftet med införandet av ett system med transaktionskonto är att försvåra för enskilda och företag att få utbetalningar på felaktiga grunder. Om endast statliga myndigheter och arbetslöshetskassorna omfattas av systemet

2018-08-27

Dnr SN/2018:328

ser socialnämnden, liksom de kommuner som utredningen har varit i kontakt med, en risk för en övervältringseffekt, där oseriösa aktörer riktar in sig på kommunal verksamhet när det blir svårare att få ut medel från de statliga välfärdssystemen. Det blir extra problematiskt då många kommuner inte har förutsättningar att bygga upp kontrollfunktioner som kan förebygga och upptäcka felaktigheter.

Utredningen föreslår en fortsatt utredning av förutsättningarna för kommunal och regional anslutning till systemet med transaktionskonto. Socialnämnden välkomnar en sådan utredning, och framhåller att det är av vikt att den genomförs så att kommuner kan ansluta sig i samband med att myndigheten inleder sitt arbete.

Med dessa synpunkter tillstyrker socialnämnden förslaget.

Marie Lundqvist
Socialchef

Jennifer Gavin
Stöd- och utvecklingschef

Expedieras till
Kommunledningsförvaltningen
Finansdepartementet

Sammanfattning av *Kontroll för ökad tilltro – en ny myndighet för att förebygga, förhindra och upptäcka felaktiga utbetalningar från välfärdssystemet* (SOU 2020:35)

Kontrollen över utbetalningarna från välfärdssystemen bör, enligt utredningens direktiv, samordnas och stärkas. Utredningens huvudsakliga uppdrag har varit att överväga om en funktion för systemövergripande riskanalyser, urval och kontroller bör införas för att förhindra att felaktiga belopp betalas ut, och för att säkerställa att utbetalningarna sker till rätt mottagare.

Vi föreslår att en ny myndighet, Myndigheten för utbetalningskontroll, inrättas den 1 juli 2022. Myndigheten ska förebygga, förhindra och upptäcka felaktiga utbetalningar från de statliga välfärdssystemen. Verksamheten ska vara ett komplement till välfärdsmyndigheternas kontrollarbete. Ansvaret för ärendehandläggning och beslut ska ligga kvar på respektive myndighet. Våra förslag ska inte heller begränsa de kontroller som görs hos myndigheterna inom ramen för respektive förmån eller stöd. Myndigheten för utbetalningskontroll ska även administrera ett system med transaktionskonto för utbetalningar.

Syftet med våra förslag är att minska de felaktiga utbetalningarna och därigenom förebygga brottslighet som drabbar välfärdssystemen.

Förändrad problembild för felaktiga utbetalningar från välfärdssystemen

De senaste två decennierna har det skett stora förändringar i samhället med betydelse för välfärdssystemen. Samhället i stort har digitaliserats och så även välfärden. Rörligheten av arbetskraft mellan länderna har ökat liksom inslaget av privata utförare i välfärdssystemen. Dessa förändringar har fört med sig en rad konsekvenser. En negativ konsekvens är att det har skapat förutsättningar för ett mer sofistikerat och medvetet missbruk av välfärdssystemen. Där problembilden tidigare i stor utsträckning handlade om enskilda individers fusk, exempelvis kolliderande utbetalningar, ser vi i dag en helt annan typ av upplägg som drabbar välfärden. Företag och identitetsmissbruk används som verktyg för att felaktigt få utbetalningar från välfärdssystemen. Det stora flertalet företag i välfärden är seriösa, men svårigheten är att upptäcka de företag som används för att missbruka välfärdssystemen. Digitaliseringen har skapat stordriftsfördelar för identitetsmissbruk som tidigare inte fanns.

De som systematiskt utnyttjar välfärdssystemens svaga punkter är något av experter på det. De rör sig mellan välfärdssystemen, och hittar och utnyttjar snabbt luckor i regelverk och kontroller. Myndigheterna har inte möjlighet till samma flexibilitet. Det beror bl.a. på begränsningar i regelverken och på bristande möjligheter att snabbt kommunicera information om nya upplägg. Dessutom gör komplexiteten att det många gånger krävs ett omfattande utredningsarbete för att identifiera och motverka ett brottsligt utnyttjande.

De nya sätten att utnyttja systemen ställer därför nya krav på välfärdsmyndigheterna. Det är svårare att upptäcka, utreda och åtgärda upplägg som omfattar flera personer och där mer än en myndighet kan vara berörd. Sett till välfärdssystemen som en helhet är den samlade beredskapen för att stävja dessa upplägg inte tillräcklig. Många gånger finns de uppgifter som skulle behövas för att upptäcka felaktigheter hos en annan myndighet. Det kan vara så att den beslutande myndigheten inte har

tillgång till uppgiften eller inte får använda den för att upptäcka och förhindra felaktiga utbetalningar på grund av sekretessregler och bestämmelser om behandling av personuppgifter. Det saknas möjligheter att i den utsträckning som behövs använda data från olika delar av välfärdssystemen om utbetalningar, intyg och andra kontrolluppgifter, eller uppgifter från Skatteverket, för att effektivt upptäcka och förhindra felaktiga utbetalningar.

Myndigheterna har också olika förutsättningar för att bedriva sin kontrollverksamhet. Kontrollfrågorna prioriteras olika hos olika myndigheter och prioriteringen har växlat över tid. Det gör att långsiktigheten i kontrollfrågan uteblir och att kontrollinsatserna kan uppfattas som ryckiga. Myndigheterna lägger ner ett omfattande arbete på att motverka felaktiga utbetalningar, men alla myndigheter utgår från den egna verksamheten. Ingen har till uppdrag eller ens möjlighet att arbeta mot felaktiga utbetalningar utifrån välfärdssystemen som helhet.

Allt detta bidrar till att de som systematiskt vill utnyttja systemen tenderar att ständigt ligga steget före medan myndigheterna ligger steget efter i sitt kontrollarbete.

Myndigheternas kontrollarbete behöver kompletteras

För att komma åt de avancerade uppläggen som drabbar välfärdssystemen behövs nya metoder. Vi menar att nästa steg i uppbyggnaden av försvaret mot de systematiska uppläggen som riktas mot välfärden är att skapa gemensamma strukturer som kan bemöta dessa. För att kunna motverka felaktiga utbetalningar behöver välfärdssystemen ses som ett sammanhängande system. Det krävs långsiktighet, kontinuitet och ett sammanhållet kontrollarbete för välfärdssystemen som helhet.

Det är därför vår uppfattning att det ska inrättas en särskild myndighet som utifrån ett helhetsperspektiv ska verka för att motverka felaktiga utbetalningar och missbruk av välfärdssystemen. Detta innebär att arbetet med att motverka felaktiga utbetalningar får stå i fokus och inte behöver konkurrera med andra uppgifter. En ny myndighet är en tydlig signal om att regeringen prioriterar frågan om att motverka felaktiga utbetalningar från välfärdssystemen. Myndigheten kan också ha en förebyggande effekt. Vidare kan en myndighet med ett utpekat ansvar för dessa frågor bidra till att utveckla samverkan på området. Detta kommer sammantaget att leda till minskad brottslighet och stärkt tilltro till välfärdssystemen.

Våra förslag rör de centrala delarna av de statliga välfärdssystemen där det är särskilt viktigt att det finns ett förtroende för systemen. Därför omfattas utbetalningar från Arbetsförmedlingen, Centrala studiestödsnämnden (CSN), Försäkringskassan och Pensionsmyndigheten av myndighetens uppdrag att förebygga, förhindra och upptäcka felaktiga utbetalningar. Även Skatteverket omfattas av förslagen och i vissa delar också arbetslöshetskassorna. Dessutom ska flera andra myndigheter lämna uppgifter till Myndigheten för utbetalningskontroll och ta emot underrättelser om felaktigheter.

Ett system med transaktionskonto

För att skapa en samlad struktur för utbetalningar från de statliga välfärdssystemen och Skatteverket föreslår vi att ett system med transaktionskonto inrättas. Systemet ska administrera utbetalningar från välfärdssystemen och Skatteverket. En samlad funktion, separat från andra myndigheter, innebär en överblick över välfärdens utbetalningar som helhet samtidigt som risken för att uppgifter sprids till fler än nödvändigt begränsas.

Transaktionskontosystemet leder till en effektivisering för staten som helhet bl.a. genom att utbetalningar från välfärdssystemen kan hanteras samlat och att kontouppgifter för mottagare av utbetalningar bara behöver administreras av en myndighet i stället för av flera. Systemet med transaktionskonto ska regleras i en särskild lag och en kompletterande förordning.

Uppgifter från transaktionskontosystemet ska utgöra grunden för myndighetens arbete med dataanalyser och urval för att upptäcka och förhindra felaktiga utbetalningar.

Dataanalyser och urval

Myndigheten för utbetalningskontroll ska göra dataanalyser och urval för att upptäcka felaktiga utbetalningar från välfärdssystemen. Det handlar om sådant som de beslutande myndigheterna har svårt att upptäcka utifrån den data som de var för sig har tillgång till. Fokus för verksamheten vid Myndigheten för utbetalningskontroll ska vara avsiktliga fel och mer avancerade upplägg som drabbar välfärdssystemen där någon eller några på oriktiga grunder vill tillskansa sig medel. Möjligheten att samköra uppgifter från olika välfärdsmyndigheter gör att myndigheten kan upptäcka felaktigheter på ett sätt som inte går i dag. Det gäller särskilt i de fall där uppgifter som indikerar felaktigheter finns hos en annan än den beslutande myndigheten. Det gör det även möjligt att jämföra uppgifter som lämnats till olika myndigheter och på så sätt upptäcka felaktigheter.

Som underlag för dataanalyser och urval behöver myndigheten, utöver uppgifter om utbetalningar från transaktionskontosystemet, använda vissa uppgifter från beslutande myndigheter såsom beslut, intyg från arbetsgivare och lämnade kontaktuppgifter. Därtill ska vissa andra uppgifter från myndigheter ligga till grund för dataanalyserna och urvalen såsom registeruppgifter från Bolagsverket och Kronofogdemyndigheten. Även Skatteverkets uppgifter på individnivå i arbetsgivardeklarationer och vissa skatteuppgifter samt folkbokföringsuppgifter ska få användas. Vidare ska vissa uppgifter från arbetslöshetskassorna kunna användas.

Granskningar

Urvalsträffar från myndighetens dataanalyser och urval behöver hanteras och sorteras för att kunna utgöra ett effektivt underlag i välfärdsmyndigheternas arbete med att upptäcka och förhindra felaktiga utbetalningar från välfärdssystemen. Vi föreslår att detta ska kunna ske i två steg, inledande och fördjupad granskning. Myndighetens granskning av urvalsträffar ska regleras i en särskild lag.

Inledande granskning innebär hantering och sortering av samtliga urvalsträffar som lämnas över från verksamheten med dataanalyser och urval. För vissa urvalsträffar kan det vara motiverat att myndigheten vidtar en fördjupad granskning, dvs. en kompletterande utredning. Fördjupad granskning får inledas när det finns anledning att anta att det har skett en felaktig utbetalning. Urvalsträffar där det är troligt att fler än en myndighet eller arbetslöshetskassa berörs bör prioriteras. Vid en fördjupad granskning ska myndigheten kunna hämta in kompletterande underlag.

Myndigheten för utbetalningskontroll ska underrätta andra myndigheter och arbetslöshetskassor om resultatet av granskningarna. Granskningarna ska utgöra ett stöd för beslutande myndigheters och arbetslöshetskassors kontrollarbete. Myndigheten för utbetalningskontroll ska inte ompröva eller överpröva andra myndigheters beslut.

Stödja och följa

Myndigheten för utbetalningskontroll ska stödja och följa statliga myndigheters och arbetslöshetskassors arbete med att motverka felaktiga utbetalningar från välfärdssystemen. Det finns mycket att vinna på kunskapsutbyte, gemensamma problemanalyser och samordnade åtgärder. Myndigheten för utbetalningskontroll ska utgöra en plattform för myndighetsgemensamt arbete med att motverka felaktiga utbetalningar. Uppdragets närmare utformning bör lämnas till myndigheten.

Myndigheten kan, genom sin särskilda kompetens i kontrollfrågor, bli en viktig remissinstans vid reformer av välfärdssystemen. Detta är särskilt viktigt vid stora eller snabba förändringar som gör att det kan uppstå nya möjligheter för de som systematiskt vill tillskans sig medel på oriktiga grunder. Myndigheten ska också ha i uppdrag att vart tredje år lämna en samlad redogörelse till regeringen om arbetet mot felaktiga utbetalningar. Redogörelsen ska utgöra ett underlag i arbetet med att motverka felaktiga utbetalningar från välfärdssystemen.

Dessutom anser vi att det ska fastslås ett mål om att felaktiga utbetalningar ska minska. Målet ska följas upp i budgetpropositionen.

Personuppgiftsbehandling

Den behandling av personuppgifter som ska ske i myndighetens verksamhet, särskilt vid dataanalyser och urval, utgör ett intrång i enskildas personliga integritet. Vi menar att integritetsintrånget står i proportion till syftet att kunna upptäcka och förhindra felaktiga utbetalningar från välfärdssystemen och därigenom motverka välfärdsbrottslighet. Vi föreslår en lag som reglerar och möjliggör den personuppgiftsbehandling som är nödvändig för att myndigheten ska kunna utföra föreslagna uppdrag. Förslagen omfattar ett antal skyddsåtgärder, bl.a. sökbegränsningar, begränsningar av tillgången till personuppgifter för myndighetens personal och regler om åtkomstkontroll.

I förordning ska det anges vilka uppgifter Myndigheten för utbetalningskontroll ska få använda vid dataanalyser och urval. Detta för att säkerställa principen om uppgiftsminimering och för att stärka skyddet för den personliga integriteten.

Offentlighet och sekretess

Det finns behov av sekretessregler till skydd för såväl enskilda som allmänna intressen i myndighetens verksamhet. Absolut sekretess ska gälla för uppgifter om enskildas personliga och ekonomiska förhållanden i myndighetens verksamhet. Uppgifterna kommer alltså alltid att vara sekretessbelagda och får inte lämnas ut till myndigheter och andra, om det inte finns sekretessbrytande bestämmelser som tillåter det. Vi föreslår också att det ska finnas möjlighet att sekretessbelägga uppgifter om metoder, modeller och riskfaktorer hänförliga till analyser och urval för att förebygga, förhindra och upptäcka felaktiga utbetalningar från välfärdssystemen.

Myndighetens verksamhet förutsätter informationsutbyte med andra myndigheter och aktörer. Vi föreslår sekretessbrytande underrättelse- och uppgiftsskyldigheter för att möjliggöra detta informationsutbyte. Förslagen innebär att Arbetsförmedlingen, Bolagsverket, CSN, Försäkringskassan, Inspektionen för vård och omsorg, Migrationsverket, Pensionsmyndigheten, Skatteverket och arbetslöshetskassorna ska lämna vissa närmare angivna uppgifter till myndighetens verksamhet med dataanalyser och urval. Statliga myndigheter, arbetslöshetskassor och kreditinstitut ska lämna uppgifter avseende en namngiven fysisk eller juridisk person som är av betydelse för myndighetens fördjupade granskningar.

Lagen om underrättelseskyldighet vid felaktiga utbetalningar från välfärdssystemen (2008:206) ska gälla för Myndigheten för utbetalningskontroll. Myndigheten kan också upptäcka andra troliga felaktigheter i myndigheters beslut och registreringar. Bolagsverket, Inspektionen för vård och omsorg, Migrationsverket och Skatteverket ska därför underrättas när granskningar visar på felaktigheter i deras beslut eller register.

Myndigheten för utbetalningskontroll

Myndigheten ska organiseras som en styrelsemyndighet. Lokalisering av myndigheten bör ske med närhet till en större arbetsmarknadsregion och med närhet till en universitets- eller högskoleort.

Inom myndigheten ska det finnas ett integritetsskyddsråd med uppgift att utöva fortlöpande insyn i de åtgärder som vidtas för att säkerställa integritetsskyddet i verksamheten.

Myndighetens uppdrag beräknas kräva en bemanning på 80 årsarbetskrafter när verksamheten är fullt utbyggd efter tre år.

Verksamheten ställer höga krav på informationssäkerhet och skyddsåtgärder.

Väl fungerande samverkan är en förutsättning för myndighetens verksamhet

Myndigheten för utbetalningskontroll ska särskilt samverka med Arbetsförmedlingen, CSN, Försäkringskassan, Migrationsverket, Pensionsmyndigheten och Skatteverket i syfte att motverka felaktiga utbetalningar. Motsvarande uppdrag skrivs in i respektive samverkande myndighets instruktion. I instruktionen för Myndigheten för utbetalningskontroll anges även att myndigheten ska samverka med andra berörda parter.

Myndigheten för utbetalningskontroll bör delta i myndighetssamverkan mot organiserad brottslighet som nätverksmyndighet.

Vissa övriga frågor

Utredningen har även haft i uppdrag att överväga om kommuner frivilligt ska kunna ansluta sig till funktionen, kartlägga för- och nackdelar för enskilda med ett samordnat uppgiftslämnande samt utreda om funktionen bör ta över ansvaret för att driva in beslutade återkravsärenden från beslutande myndigheter.

Omfattning och beskaffenhet av felaktiga utbetalningar inom den kommunala välfärden är inte tillräckligt belagt. Problembilden tycks likna den som finns för de statliga välfärdsutbetalningarna. Flera stora skillnader finns dock mellan statliga och kommunala utbetalningar inom välfärden, varför möjligheten för kommuner att ansluta sig till de funktioner som Myndigheten för utbetalningskontroll ansvarar för bör utredas vidare. Även möjligheten för regionerna att ansluta sig till dessa funktioner bör utredas.

Transaktionskontosystemet innebär en förenkling för enskilda genom att kontouppgifter för utbetalningar endast behöver lämnas en gång och till en myndighet. I övrigt har vi inte kunnat identifiera behov av att Myndigheten för utbetalningskontroll ska samordna ytterligare uppgiftslämnande från enskilda.

Överväganden om att samla hanteringen av återkravsfordringar vid Myndigheten för utbetalningskontroll bör göras först efter att vissa regelförändringar på området är genomförda och har fått effekt. Det gäller bl.a. regler för bostadsbidrag som utgör majoriteten av återkraven hos Försäkringskassan.

Finansiering av förslagen

Vårt huvudförslag är att det tillförs medel så att finansieringen inte tas från befintliga verksamheter på välfärdsområdet. Ett alternativt förslag är att finansieringen sker genom att minska förvaltningsanslagen för de berörda myndigheterna. Det bör då göras genom en generell sänkning av anslaget för de myndigheter som ska omfattas av systemet med transaktionskonto. Neddragningen bör vara proportionerlig i förhållande till myndigheternas driftkostnader. De myndigheter vi föreslår ska anslutas till transaktionskontosystemet, och som alltså påverkas av finansieringsförslaget, är Arbetsförmedlingen, CSN, Försäkringskassan, Pensionsmyndigheten och Skatteverket.

De totala kostnaderna för en fullt utbyggd verksamhet beräknas till omkring 153 miljoner kronor per år. Kostnader för bankavgifter kommer att minska för berörda myndigheter och motsvarande anslag bör flyttas till anslaget för Myndigheten för utbetalningskontroll. Det kvarstående finansieringsbehovet för en fullt utbyggd verksamhet är 120 miljoner kronor.

Ett snabbt genomförande

Det är angeläget att våra förslag genomförs så snart som möjligt så att Myndigheten för utbetalningskontroll kan påbörja sin verksamhet. Arbetet med att förebygga, förhindra och upptäcka felaktiga utbetalningar från välfärdssystemen är en fråga som måste ha hög prioritet. Vi föreslår att myndigheten ska inleda sin verksamhet den 1 juli 2022. De nya lagarna och förordningarna ska träda i kraft när myndigheten inleder sitt arbete.

Anslutningen av myndigheternas utbetalningar till transaktionskontot ska ske successivt och senast den 1 juli 2025 ska alla berörda utbetalningar ske via transaktionskontosystemet.

Konsekvenser av förslagen

Färre felaktiga utbetalningar och minskad välfärdsbrottslighet Vi bedömer att förslagen leder till minskade felaktiga utbetalningar och därigenom minskad välfärdsbrottslighet. Framst bedömer vi att förslagen kan påverka avsiktliga fel samt systematiska och organiserade upplägg som riktas mot välfärdssystemen.

Våra förslag kommer att leda till tidigare upptäckter av felaktiga utbetalningar än i dag. Snabbare upptäckt medför väsentligt större möjligheter att genom återkrav få tillbaka felaktiga utbetalningar. Genom dataanalyser och urval kommer Myndigheten för utbetalningskontroll att upptäcka felaktigheter som i dag förblir oupptäckta. Även myndighetens möjlighet att sambearbeta folkbokföringsuppgifter med uppgifter från välfärdssystemen gör att identitetsmissbruk kommer att upptäckas i större omfattning.

Myndighetens granskningar innebär en ytterligare aktör som komplement till de befintliga myndigheternas arbete med att granska felaktigheter, särskilt avseende avancerade upplägg som drabbar mer än ett välfärdssystem. Det kan röra sig om företag som används som brottsverktyg och

identitetsmissbruk som i dag är svåra att upptäcka eftersom enskilda myndigheter saknar tillgång till de uppgifter som behövs för att upptäcka och utreda dessa upplägg.

Att fler felaktigheter upptäcks kommer också att öka möjligheterna att lagföra brottslighet. Tidigare upptäckt av felaktigheter leder till att kommande utbetalningar kan förhindras då löpande utbetalningar kan stoppas i ett tidigare skede. Attraktiviteten i denna brottslighet kan därför förväntas minska.

En viktig aspekt av minskad brottslighet som drabbar välfärdssystemen är att det kan ha betydelse för annan, ännu grövre brottslighet. Det finns exempel på att pengar från välfärdsbrottslighet använts till att finansiera grov organiserad brottslighet och i vissa fall även terroristverksamhet. Våra förslag minskar möjligheterna att finansiera sådan allvarlig brottslighet, vilket innebär positiva effekter för samhället i stort.

Vi menar att våra förslag kommer att leda till en ökad tilltro till såväl välfärden som samhällsinstitutionerna.

Lägre utgifter för staten på sikt

Förslagen kommer initialt att innebära ökade utgifter, men på sikt bedöms de leda till lägre utgifter för staten. Nettoeffekten beror på de resultat som den föreslagna verksamheten uppnår när det gäller minskade felaktiga utbetalningar.

De felaktiga utbetalningarna från välfärdssystemen har uppskattats till cirka 18 miljarder kronor, motsvarande cirka 3 procent av de totala utbetalningarna. Trots att skattningarna ska tolkas med försiktighet, kan man utgå från att de felaktiga utbetalningarna uppgår till betydande belopp. Även om bara en mindre andel av de totala felaktiga utbetalningarna försvinner väger det upp och motiverar kostnaderna för myndigheten.

Transaktionskontosystemet innebär i stort sett en fast kostnad. Övriga delar av förslagen kan i större utsträckning anpassas efter vald ambitionsnivå.

Konsekvenser för statliga myndigheter

Flera av konsekvenserna för de statliga myndigheterna kommer att vara likartade. En konsekvens för de direkt berörda myndigheterna är att it-lösningar behöver anpassas för överföring av data till Myndigheten för utbetalningskontroll. De berörda myndigheterna påverkas också genom det samarbete som byggs upp med Myndigheten för utbetalningskontroll. De underrättelser om misstänkta felaktigheter som lämnas från Myndigheten för utbetalningskontroll ska kunna tas till vara på de befintliga myndigheterna. Förslagen bidrar till kvaliteten i myndigheternas kontrollarbete. Underrättelserna från Myndigheten för utbetalningskontroll kommer sannolikt att leda till fler omprövnings- och återkravsärenden hos de berörda myndigheterna.

Konsekvenser för kommuner och regioner

Förslagen innebär inga konsekvenser för den kommunala självstyrelsen då kommuner och regioner inte föreslås omfattas av myndighetens verksamhet i detta skede. Det finns dock en risk för övervältring. Om arbetet mot felaktiga utbetalningar inom statliga verksamheter förstärks kan det

leda till att de som missbrukar systemen i större utsträckning inriktar sig på regionala eller kommunala verksamheter.

Konsekvenser för arbetslöshetskassor

Arbetslöshetskassorna ska kontinuerligt lämna uppgifter till Myndigheten för utbetalningskontroll. Förslaget innebär därmed en något ökad uppgiftslämnarbörda för arbetslöshetskassorna.

Arbetslöshetskassorna kommer regelbundet att få underrättelser från Myndigheten för utbetalningskontroll om misstänkta felaktigheter som ska hanteras av arbetslöshetskassorna. På så sätt får arbetslöshetskassorna underlag som kan användas i deras kontrollarbete.

Konsekvenser för företag

Förslaget bidrar till konkurrens på lika villkor. Seriösa aktörer upplever i dag svårigheter att hävda sig i konkurrensen med företag som har en affärskalkyl som bygger på att missbruka välfärdssystemen. Våra förslag syftar till att särskilt försvåra för de mer allvarliga uppläggen som drabbar välfärdssystemen.

Kreditinstitut kommer att få en något ökad uppgiftslämnarbörda eftersom de föreslås bli skyldiga att lämna uppgifter till myndighetens verksamhet med fördjupade granskningar.

Länk till remissen

<https://www.regeringen.se/4a4bdb/contentassets/d62c8a6857ab49e4b21111009897f819/kontroll-for-okad-tilltro--en-ny-myndighet-for-att-forebygga-forhindra-och-upptacka-felaktiga-utbetalningar-fran-valfardssystemen-sou-202035.pdf>



4

Granskning av intrångsskydd och IT-säkerhet i verksamhetssystem - Botkyrka kommun 2020-rapport KS/2020:444 (SN 2020:384)

Beslut

Socialnämnden godkänner förvaltningens yttrande och överlämna det till kommunens revisorer.

Ärendet

På uppdrag av de förtroendevalda revisorerna i Botkyrka kommun har PwC genomfört en informationssäkerhetsgranskning avseende tre förvaltningars IT-system, varav ett var socialförvaltningens verksamhetssystem Procapita.

Nämnderna ska ha lämnat sina svar utifrån rapporten till kommunens revisorer senast 2020-10-31.



2020-10-01

Dnr SN/2020:384

Referens

Eva Thede, Enhetschef IT-sektionen
Stöd- och utvecklingsenheten

Mottagare

Socialnämnden
Kommunens förtroendevalda revisorer

Granskning av intrångsskydd och IT-säkerhet i verksamhetssystem - Botkyrka kommun 2020-rapport KS/2020:444

Förslag till beslut

Socialnämnden föreslås besluta att godkänna yttrandet och överlämna det till kommunens revisorer.

Ärendet

På uppdrag av de förtroendevalda revisorerna i Botkyrka kommun har PwC genomfört en informationssäkerhetsgranskning avseende tre förvaltningars IT-system, varav ett var socialförvaltningens verksamhetssystem Procapita.

Nämnderna ska ha lämnat sina svar utifrån rapporten till kommunens revisorer senast 2020-10-31.

Bakgrund

PwC har på uppdrag av de förtroendevalda revisorerna i Botkyrka kommun genomfört en granskning avseende intrångsskydd och IT-säkerhet i verksamhetssystem hos Vård- och omsorgsnämnden, Socialnämnden och Utbildningsnämnden. Granskningen bestod i att se om nämnderna har säkerställt att informationshanteringen håller en tillräcklig och tillfredsställande nivå för att reducera risker för obehörig åtkomst. Efter genomförd granskning är PwCs bedömning att Botkyrka kommun ej har säkerställt att informationshanteringen håller en tillräcklig och tillfredsställande nivå för att reducera risken för obehörig åtkomst.

Nedan redovisas de fyra rekommendationer som framgått i revisionen och de åtgärder som bedöms behöver vidtas gällande socialförvaltningens verksamhetssystem Procapita.

- 1. Vi rekommenderar att kommunens nämnder upprättar ett styrdokument för hur dokument löpande ska revideras och versionshanteras. Det rekommenderas även att de nämnder som saknar styrdokument för informationshantering, upprättar dessa för befintliga system.*

Revisionen visar att detta är delvis uppfyllt gällande Procapita. Socialförvaltningen har en informationshanteringsplan som beskriver hur information övergripande ska hanteras i alla olika system som finns inom förvaltningen. Det finns också en mängd styrdokument och

2020-10-01

Dnr SN/2020:384

enhetsanpassade guider som täcker in större delen av hanteringen/handläggningen i Procapita. Det som saknats tidigare är att visa att dokumentation uppdateras kontinuerligt och versionshanteras. Alla ändringar i dokument och riktlinjer har nu börjat versionhanteras för att leva upp till rekommendationen. För att säkerställa att dokumentationen gällande rutiner och processer är uppdaterade och löpande revideras enligt god praxis föreslås det läggas som kontrollmoment i internkontrollplanen att se över och uppdatera all dokumentation gällande informationshantering i Procapita.

2. *PwC rekommenderar att man säkerställer att kommunens varje användare har genomgått utbildning i systemet och det görs löpande åtminstone 1 gång om året.*

Revisionen visade att detta var delvis uppfyllt för Procapita men att det saknades kontroll över att nya handläggare tagit del av den utbildning och information som finns gällande informations-säkerhet. Åtgärd för detta är redan genomförd i och med det sedan sommaren är etablerad rutin att skicka en digital nanoutbildning till alla nya medarbetare som de måste genomföra innan de får tillgång och kan arbeta i Procapita. Utbildningen tar bland annat upp en del säkerhetsrelaterade element, som regler för inloggning och sekretess. Systemförvaltare kontrollerar sedan tekniskt att medarbetaren har genomgått utbildningen, och hur lång tid det tog, innan behörigheten slås på. Ett samarbete mellan systemförvaltare av Procapita och förvaltningens dataskyddsbud har påbörjats för att med stöd av ett årshjul följa upp att alla användare har tillräcklig information för att på ett säkert sätt arbeta i systemet.

3. *PwC rekommenderar att Botkyrka utbildar systemförvaltarna och upprättar en guide för hur dem rutinmässigt kan ställa krav mot leverantören för att kontrollera att avtalade rutiner uppfylls som t.ex. Backup, restore, spårbarhet och intrångstester.*

Revisionen visar att det finns bra rutiner hos leverantören Tieto men det finns en kompetensbrist hos förvaltningen/systemförvaltare över vilka krav som behöver ställas mot leverantören. Under våren 2020 beslutade Strategisk grupp organisationsutveckling (SGO) om en ny modell för leverantörsstyrning som utgår ifrån att IT-enheten kommer ta större ansvar i kontakten med leverantörerna och har ansvar för att framöver stödja förvaltningarna i detta arbete. Tidigare låg allt ansvar på de enskilda förvaltningarna som de facto inte besitter den tekniska kompetensen som krävs för att kunna ställa rätta krav på leverantören. Bedömningen är att det förändrade arbetssättet där IT-enheten tar större ansvar kommer leda till en kompetenshöjning hos systemförvaltarna och att adekvata krav kommer ställas på leverantören. Rutiner kommer tas fram tillsammans med IT-enheten för att säkerställa att intrång- och säkerhetstester genomförs regelbundet. Implementering av det nya arbetssättet mellan förvaltningarna och IT-enheten kommer ske under hösten 2020

4. *PwC rekommenderar att förvaltningen dokumenterar beroendet mellan systemet och stödsystemen, för att uppmärksamma eventuella sårbarheter i behörighets hanteringen, så en säker behörighetskontroll kan säkerställas.*

2020-10-01

Dnr SN/2020:384

Det framgår i revisionen att det finns bra rutiner för att se till att ingen obehörig har tillgång till information i Procapita som den inte har rätt till. Till exempel finns samarbete med Lönekontoret som varje månad skickar listor på de som avslutat sin anställning och dokumentation som visar alla anställdas roller och behörigheter. En planerad åtgärd är att sammanställa de rutiner som finns till ett och samma dokument så att det blir tydligare. Det finns också behov att dokumentera och implementera rutin för hur det går till när en anställd byter enhet, och behöver få ny behörighet, eftersom detta ofta missas att anmälas från närmaste chef till systemförvaltare. Åtgärderna är planerade att vara genomförda till den sista november 2020.

Socialnämndens yttrande

Socialnämnden har i yttrandet presenterat de åtgärder som redan har och ska genomföras, för att komma till rätta med de brister som uppdagats och har inget ytterligare att tillägga till revisionskrivelsen.

Expedieras till

Kommunens revisorer

Utbildningsnämnden
Vård- och omsorgsnämnden
Socialnämnden

Granskning av intrångsskydd och IT-säkerhet i verksamhetssystem

PwC har på uppdrag av de förtroendevalda revisorerna i Botkyrka kommun genomfört en granskning avseende intrångsskydd och IT-säkerhet i verksamhetssystem. bedöma om Vård- och omsorgsnämnden, Socialnämnden och Utbildningsnämnden har säkerställt att informationshanteringen håller en tillräcklig och tillfredsställande nivå för att reducera risker för obehörig åtkomst för tre utvalda IT-system; Socialnämndens system Procapita, Utbildningsnämndens system Vklass och Vård- och omsorgsnämndens system Phoniro Care.

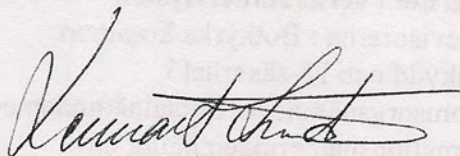
Efter genomförd granskning är vår bedömning att Botkyrka kommun **ej har säkerställt** att informationshanteringen håller en tillräcklig och tillfredsställande nivå för att reducera risken för obehörig åtkomst. Till grund för vår bedömning ligger iakttagelser och bedömningar av sex kontrollfrågor, vilka redovisas i rapporten

Mot bakgrund av noterade iakttagelser och genomförd granskning lämnar vi följande rekommendationer:

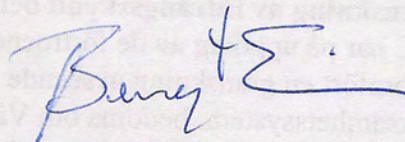
- Vi rekommenderar att kommunens nämnder upprättar ett styrdokument för hur dokument löpande ska revideras och versionshanteras. Det rekommenderas även att de nämnder som saknar styrdokument för informationshantering, upprättar dessa för befintliga system.
- Vi rekommenderar att man säkerställer att kommunens samtliga användare har genomgått utbildning i systemet och det görs löpande åtminstone 1 gång om året.
- Vi rekommenderar att Botkyrka utbildar systemförvaltarna och upprättar en guide för hur de rutinmässigt kan ställa krav mot leverantören för att kontrollera att avtalade rutiner uppfylls som t.ex. Backup, restore, spårbarhet och intrångstester.
- Vi rekommenderar att det upprättas dokumentation över beroendet mellan systemet och stödsystemen, för att uppmärksamma eventuella sårbarheter i behörighetshanteringen, så att en säker behörighetskontroll kan säkerställas.

Revisorerna översänder rapporten till utbildningsnämnden, vård- och omsorgsnämnden samt socialnämnden för svar. Svaret ställs till kommunens revisorer och ska vara revisorerna tillhanda senast den 2020-10-31.

För kommunens revisorer



Lennart Lindström
Ordförande



Bengt Ericson
Vice ordförande

För kännedom
Kommunfullmäktiges presidium
Kommunledning
Politiska sekreterare

Granskning av intrångsskydd och it- säkerhet i verksamhetssystem

Botkyrka kommun

Julius Widén

Anna Magnusson

Mattias Gröndahl

Robin Rosenberg



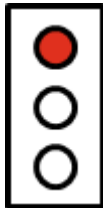
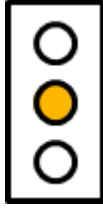
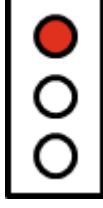
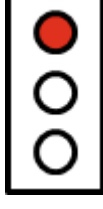
Innehållsförteckning

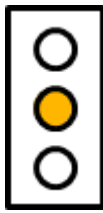
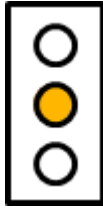
Sammanfattning	1
Inledning	4
Bakgrund	6
Syfte och revisionsfrågor	6
Revisionskriterier	6
Avgränsning	6
Metod	4
Faktiskt genomförande	4
lakttagelser och bedömningar	5
Kontrollfråga 1	6
Kontrollfråga 2	6
Kontrollfråga 3	7
Kontrollfråga 4	9
Kontrollfråga 5	10
Kontrollfråga 6	11
Slutsats	12
Rekommendationer	13
Bilagor	16
Intervjuer	16
Dokumentation	16
Bedömningsskala	17

Sammanfattning

Granskningen avser att bedöma om Vård- och omsorgsnämnden, Socialnämnden och Utbildningsnämnden har säkerställt att informationshanteringen håller en tillräcklig och tillfredsställande nivå för att reducera risker för obehörig åtkomst för tre utvalda IT-system; Socialnämndens system Procapita, Utbildningsnämndens system Vklass och Vård- och omsorgsnämndens system Phoniro Care.

Efter genomförd granskning är vår bedömning att Botkyrka kommun **ej har säkerställt** att informationshanteringen håller en tillräcklig och tillfredsställande nivå för att reducera risken för obehörig åtkomst. Till grund för vår bedömning ligger iakttagelser och bedömningar av sex kontrollfrågor, vilka redovisas i rapporten.

Kontrollmål	Bedömning
Kontrollfråga 1 Är befintlig dokumentation gällande rutiner och processer kopplade till informationshanteringen, uppdaterad och löpande reviderad enligt god praxis?	
Kontrollfråga 2 Har användarna av systemen en god förståelse om de rådande rutinerna gällande säkerheten av systemen, och säkerställer kommunen att det efterlevs?	
Kontrollfråga 3 Har kommunen en process för kontinuerlig behörighetskontroll för att säkerställa rätt behörigheter i systemen?	
Kontrollfråga 4 Är möjligheten till återställning av systemen vid en incident kontinuerligt testad och dokumenterad?	

<p>Kontrollfråga 5</p> <p>Finns det tillräcklig loggning av systemen för att i efterhand få full spårbarhet till vem som har haft tillgång till systemet?</p>	
<p>Kontrollfråga 6</p> <p>Är den tekniska säkerheten för systemen på en tillräckligt god nivå för att säkerställa att informationen är skyddad?</p>	

Rekommendationer

Mot bakgrund av noterade iakttagelser och genomförd granskning lämnar vi följande rekommendationer:

- PwC rekommenderar att kommunens nämnder upprättar ett styrdokument för hur dokument löpande ska revideras och versionshanteras. Det rekommenderas även att de nämnder som saknar styrdokument för informationshantering, upprättar dessa för befintliga system.
- PwC rekommenderar att man säkerställer att kommunens varje användare har genomgått utbildning i systemet och det görs löpande åtminstone 1 gång om året.
- PwC rekommenderar att Botkyrka utbildar systemförvaltarna och upprättar en guide för hur de rutinmässigt kan ställa krav mot leverantören för att kontrollera att avtalade rutiner uppfylls som t.ex. Backup, restore, spårbarhet och intrångstester.
- PwC rekommenderar att förvaltningen dokumenterar beroendet mellan systemet och stödsystemen, för att uppmärksamma eventuella sårbarheter i behörighets-hantering, så att en säker behörighetskontroll kan säkerställas.

Inledning

Bakgrund

Av kommunallagen och god revisionssed följer att revisorerna årligen ska granska styrelser, nämnder och fasta fullmäktigeberedningar.

Kommunstyrelse och nämnder ska förvalta och genomföra verksamheten i enlighet med fullmäktiges uppdrag, lagar och föreskrifter. För att fullgöra uppdraget måste respektive organ bygga upp system och verktyg för ledning, styrning, uppföljning, kontroll och rapportering samt säkerställa att dessa verktyg tillämpas på avsett sätt. En bristfällig styrning och kontroll kan riskera att verksamheten inte bedrivs och utvecklas på avsett sätt.

Revisorerna har uppmärksammat att risker och hot från det framväxande digitala landskapet, cyberrisker, får ökad uppmärksamhet från både företag och myndigheter. Detta främst orsakat av de senaste årens snabba digitala utveckling med följande exponering mot internet samt ökad användning av smartphones och andra bärbara enheter hos medarbetare, både privat och i yrkeslivet. Revisorerna har under föregående år granskat såväl kommunens intrångsskydd som informationssäkerhet utifrån ett kommunövergripande perspektiv. Som ett nästa steg avser revisorerna att granska IT-styrningen i ett mer verksamhetsnära perspektiv. Granskningen avser att bedöma om Vård- och omsorgsnämnden, Socialnämnden och Utbildningsnämnden har säkerställt att informationshanteringen håller en tillräcklig och tillfredsställande nivå för att reducera risker för obehörig åtkomst för tre utvalda IT-system.

Syfte och revisionsfrågor

Har vård- och omsorgsnämnden, socialnämnden och utbildningsnämnden säkerställt att informationshanteringen håller en tillräcklig och tillfredsställande nivå för att reducera risker för obehörigt intrång?

Revisionskriterier

- Kommunallagens bestämmelser om intern kontroll
- Budget 2020
- IT-styrdokument

Avgränsning

I tid avgränsas granskningen till år 2020 och till granskningens kontrollfrågor, samt till tre utvalda system Procapita, Phoniro care och Vklass.

Metod

Granskningen genomförs utifrån tre olika områden.

- Dokumentgranskning av relevanta dokument
- Intervjuer eller workshop med personer som har kunskap om systemen
- Teknisk granskning av systemen.

Faktiskt genomförande

Granskning av informationshantering hos Botkyrka kommuns utvalda nämnder har genomförts dels genom analys av kommunens rutiner och dokumentation, dels

intervjuer med nämndernas personal och leverantörer. PwC:s intrångstester baseras på tester som återspeglar verkliga angrepp och ligger till grund för bedömning i den tekniska granskningen. Huruvida den för granskningen relevanta dokumentationen är uppdaterad och löpande revideras, att rutiner för informationshantering är väl känt bland systemens användare och nämndernas förmåga att styra systemens leverantörer har varit av särskilt intresse.

Dokumentgranskning genomfördes i följande delar:

- Dokumentation Insamling — insamling av den dokumentation som Botkyrka kommun har och som var relevant för granskningen.
- Dokumentgranskning — övergripande genomgång av den tillgängliga dokumentationen för att bilda sig en uppfattning om huruvida denna är uppdaterad och löpande revideras enligt god praxis.

Intervjuer har genomförts med:

- Personer som har kunskap om systemen (Se bilagor)
- Leverantörer av systemen (Se bilaga)

Teknisk granskning genomfördes i följande delar:

- Intervju med leverantörer - där diskuterades kryptering, backup, restore, övervakning och säkerhetstester där rutiner för dessa har kartlagts i möjligaste mån.
- Intrångstest - Tekniska tester där sårbarheter har eftersökts mot systemen.

Rapportering:

- Analys av resultatet från informationsinsamlingen, intervjuer och de tekniska testerna har sammanställts och bedömts.

Iakttagelser och bedömningar

Kontrollfråga 1

Är befintlig dokumentation gällande rutiner och processer kopplade till informationshanteringen, uppdaterad och löpande reviderad enligt god praxis?

Iakttagelser

Procapita: Det finns dokumentation gällande informationshantering och processer såsom logghantering, dataskyddsrutiner och styrdokument för informationshantering. Däremot saknas versionshantering och dokumentationen revideras inte kontinuerligt.

VKlass: En handlingsplan för informationsklassning är framtaget enligt KLASSA (KLASSA är ett självskattningsverktyg som hjälper en KLASSA sina verksamhetssystem och datalagring). Den har påbörjats tillsammans med leverantören för VKlass och finns dokumenterad. Däremot är den inte färdigställd och det saknas idag en plan för att formalisera handlingsplanen. I övrigt finns mycket lite dokumentation runt informationshantering för VKlass.

Phoniro Care: Det finns mycket begränsad dokumentation och processbeskrivningar kopplade till informationshantering för Phoniro Care. Den dokumentation som finns är mestadels generella guider om hur man använder systemet. Det finns användarmanualer och checklistor för användarna som innehåller säkerhetsrutiner för att skydda känsligt information såsom lösenordspolicy. Däremot saknas versionshantering och dokumentationen revideras inte kontinuerligt.

Bedömning

Procapita: DELVIS UPPFYLLT. Det finns dokumentation på plats, men den skulle behöva ses över kontinuerligt och en rutin för när dokumentationen ska revideras behöver fastställas.

VKlass: EJ UPPFYLLT. PwC har inte fått ta del av någon dokumentation gällande rutiner och processer kopplade till informationshantering. Många av de dokument som PwC fått ta del av saknar versionshantering. Det finns en handlingsplan framtaget enligt KLASSA, vilket är en bra grund för det fortsatta arbetet med dokumentation, men handlingsplanen är från 2018-09-11 och det går inte att utläsa om den reviderats efter det.

Phoniro Care: EJ UPPFYLLT. PwC har inte fått ta del av någon dokumentation kopplad till informationshantering för systemet och de övriga dokument som PwC fått ta del av saknar versionshantering.

Kontrollfråga 2

Har användarna av systemen en god förståelse om de rådande rutinerna gällande säkerheten av systemen, och säkerställer kommunen att det efterlevs?

Iakttagelser

Procapita: Alla användare av systemet ska gå en utbildning innan man får tillgång till systemet. Utbildningen innehåller bland annat regler för loggning och sekretess. Dessutom skickas en lathund ut till användaren med samma information och

dokumentationen finns även att tillgå på intranätet. Dock finns idag ingen kontroll eller loggning för att säkerställa att användarna har läst dokumentationen.

Socialförvaltningen har påbörjat ett arbete med att implementera "nano-utbildningar" för just detta ändamål. Arbetet har dock blivit försenat på grund av covid-19 pandemin, men man hoppas vara klar med arbetet till sommaren.

I och med att nya dataskyddsbudet tillträdde i februari 2020 har man även påbörjat ett arbete med att implementera en årscykel för informationssäkerhetsarbetet för att öka medvetenheten hos personalen. Ambitionen är att informationssäkerhetsarbetet ska bli mer systematisk. Även detta arbete är dock på paus på grund av covid-19.

VKlass: Alla verksamheter har möjlighet att få utbildning som är verksamhetsrelaterad, vilket ofta görs i grupp av en handledare men det finns idag inget formellt krav på detta. Det finns även användarguider i själva systemet som alla användare kan ta del av. Dock är de guiderna inte fokuserade på säkerhet, och det finns idag inte något sätt att säkerställa att användarna tagit del av dokumentationen.

Phoniro Care: Användarna av Phoniro Care får en grundutbildning i systemet innan man får tillgång, vilket ansvaras av enhetschefen. Där är informationssäkerhet en del av den allmänna introduktionen. IT-funktionen på förvaltningen informerar även chefer och koordinators på olika träffar, om vikten av informationssäkerhet. Mer detaljerad info finns för chefer på kommunens intranät gällande Policy för informationssäkerhet. Dock görs ingen uppföljning på utbildningen och det finns inga dokumenterade rutiner för hur utbildningen ska utföras.

Bedömning

Procapita: DELVIS UPPFYLLT. Alla användare går en utbildning innan de får tillgång till systemet. Dessutom innehåller utbildningen en del säkerhetsrelaterade element, som regler för inloggning och sekretess. Däremot saknas det kontroll på att utbildningen genomförs av alla och det sker ingen uppföljning i form av ytterligare utbildningar, till exempel årligen. Vi ser dock att åtgärder är på gång, men att det blivit försenade på grund av rådande omständigheter.

VKlass: EJ UPPFYLLT. Alla verksamheter har möjlighet att få utbildning som är verksamhetsrelaterad men det saknas fokus på informationssäkerhet. Det finns heller ingen kontroll för att säkerställa att utbildningen har genomförts av alla användare.

Phoniro Care: DELVIS UPPFYLLT. Alla ska genomföra en utbildning innan dem får tillgång i systemet, det ansvaret ligger på enhetschefen. Det finns dock inget sätt för förvaltaren att bekräfta att utbildningen genomförs.

Kontrollfråga 3

Har kommunen en process för kontinuerlig behörighetskontroll för att säkerställa rätt behörigheter i systemen?

lakttagelse

Procapita: När någon avslutar sin anställning på kommunen registreras detta i HR och lönesystemet och meddelas till förvaltningen som utför förändringen i systemet. Som kontroll skickas även en lista ut, en gång i månaden från HR till förvaltningen, med personer som har slutat och ska tas bort från systemet, dock gäller denna lista endast fast anställda och inte konsulter och timanställda. För konsulter kan man tidsbegränsa behörigheten till den period konsulten kommer arbeta på kommunen. Systemförvaltarna mailar även till chefer 2-3 gånger per år och frågar om konsulterna fortfarande arbetar på kommunen och ska ha kvar sina behörigheter. Dock är denna rutin inte dokumenterad.

Om ett konto har varit inaktivt i 90 dagar låses det automatiskt. Det syns då i systemet och man undersöker vad inaktiviteten beror på, till exempel om någon är föräldraledig.

Man anser på förvaltningen att man generellt har bra kontroll på att inga obehöriga har tillgång till systemet eller att inga användare har mer rättigheter än man ska, men det finns inga dokumenterade rutiner på detta. Vad som dokumenteras är vad varje användare har för specifik roll/roller i Procapita och vilka behörigheter som ingår i den rollen.

När en person byter tjänst och behöver andra behörigheter, läggs en ny beställning på behörighet av närmaste chef. Det har dock hänt att detta missats och det finns idag ingen del av förvaltningen som kan fånga upp misstaget. Det uppdagas som oftast av användaren själv, när personen inte har de behörigheter som krävs för att utföra sitt jobb.

VKlass: Behörigheter till VKlass är integrerat med systemet Extens. Ändringar av behörigheter sker alltså i Extens och inte direkt i VKlass. Extens synkroniserar med VKlass dagligen och om någon förändring skulle göras i VKlass, skulle den förändringen återställas när VKlass och Extens synkroniserar. PwC har inte gjort någon analys av rutiner i Extens.

Idag gör inte förvaltningen några rutinmässiga kontroller på behörigheter, om det inte har begärts av kommunen, eftersom VKlass inte är styrande och felaktigheter som uppstår ligger i bakomliggande system. Den skolledare PwC intervjuat upplever att det heller inte behövs göras kontroller, eftersom organisationen inte skulle fungera om en användare får felaktiga rättigheter, då scheman och uppgifter blir fel och det skulle uppdagas direkt.

Phoniro Care: Inga dokumenterade rutiner finns för behörighetskontroll. Rutinen för start, förändring och avslut av behörigheter ingår i chefens utbildning, dock efterlevs den rutinen inte alltid. När behörighetsbeställning inkommer IT-funktionen anges vilken behörighet användaren ska tilldelas både i systemet och gruppbehörighet i kommunens AD, dessa uppgifter skickas sedan vidare till Botkyrkas centrala IT grupp. När anställning i kommunen avslutas upphör åtkomst till systemet. IT-funktionen gör dock fortlöpande genomgångar och justeringar av behörigheter, ofta i samband med omorganisationer eller när uppdrag kommer från ansvarig chef. 1-2 gånger per år får cheferna information från förvaltningen om vikten av att ha rätt behörigheter och avsluta behörigheter, men ingen uppföljning på huruvida cheferna vidtar åtgärder görs.

Bedömning

Procapita: DELVIS UPPFYLLT. Det finns rutiner och kontroller på plats för att uppehålla en god behörighetshantering, såsom en månatlig kontroll för att säkerställa att de som avslutat sin anställning hos kommunen tas bort från systemet. Däremot är rutinen inte dokumenterad. Idag finns inget effektivt sätt för systemförvaltarna att säkerställa att de som byter tjänst inom kommunen och inte ska ha behörighet i Procapita tas bort i tid.

VKlass: EJ UPPFYLLT. Idag finns inga dokumenterade rutiner för att kontrollera behörigheter. Behörighetshanteringen av VKlass är synkroniserat med systemet Extens vilket innebär att kontrollen för kontinuerlig behörighetskontroll borde finnas för Extens snarare än VKlass. Dock är det fördelaktigt om detta finns dokumenterat för VKlass och att det följs upp av VKlass systemförvaltare och säkerställs att en sådan kontroll finns för Extens.

Phoniro Care: EJ UPPFYLLT. Idag finns inga dokumenterade rutiner för kontinuerlig behörighetskontroll. Den information som skickas ut från förvaltningens IT-funktion till chefer och koordinatörer, om vikten av behörighetskontroll är bra, men ingen uppföljning görs av huruvida cheferna vidtar åtgärder.

Kontrollfråga 4

Är möjligheten till återställning av systemen vid en incident kontinuerligt testad och dokumenterad?

lakttagelse

Procapita: Systemåterställning har enligt förvaltningen inte varit aktuellt tidigare men det finns heller inga rutiner för detta eller några krav mot leverantören på att testa eller visa något bevis på att systemåterställningen fungerar. En referens till avtalet med leverantören görs men vetskapen om vad som står i avtalet är begränsad.

Förvaltningsledaren uttrycker att man vill följa upp detta med leverantören men att det saknas kompetens på avdelningen om vad man bör fråga och vilka krav som ska ställas mot leverantören.

Enligt leverantören utför de backup enligt avtal och kan vid behov återställa systemet. Restore-tester av databasen görs minst en gång i kvartalet av leverantören. Dock har Botkyrka kommun aldrig efterfrågat dokumentation på genomförda tester.

VKlass: Det finns inga dokumenterade rutiner för kontroll av backup eller återställning för VKlass. Förvaltningen har kännedom kring leverantörens skyldigheter utifrån KLASSA verktyget, men man har begränsad vetskap av vad som står i avtalet. Förvaltningen har också begränsad kunskap internt om kravställning och vad man kan begära av leverantören.

Phoniro Care: Systemåterställning har inte varit aktuellt tidigare men det finns heller inga rutiner för detta eller några krav mot leverantören att testa eller visa något bevis på att det fungerar. Man meddelar också att detta gärna följs upp men man upplever att man inte vet vad man ska fråga efter eller hur kraven ska ställas mot leverantören. Enligt leverantören utför de backup enligt avtal och kan vid behov återställa systemet.

Leverantören gör löpande restore tester av slumpmässiga kunders databas men inte för alla kunder. Kan göras på kundens begäran, men har inte efterfrågats av Botkyrka än så länge.

Bedömning

Procapita: EJ UPPFYLLT. Det saknas rutiner för att säkerställa att en återställning av systemet är möjlig. Det saknas också kompetens hos systemförvaltarna att kravställa och följa upp leverantörens arbete. Enligt leverantören sker backuper och tester för återställning men Botkyrka kommun behöver säkerställa att detta görs genom att begära in relevanta bevis från leverantören. Det facto att leverantörerna utför rutinmässiga restore tester är självklar bra, men systemförvaltarna bör vara medvetna om detta och utmana leverantörerna att bevisa ett sådant resultat rutinmässigt.

VKlass: EJ UPPFYLLT. Det saknas rutiner för att säkerställa att en återställning av systemet är möjlig. Det saknas också kompetens hos systemförvaltarna att kravställa och följa upp leverantörens arbete. Det facto att leverantörerna utför rutinmässiga restore-tester är självklart bra, men systemförvaltarna bör vara medvetna om detta och utmana leverantörerna att bevisa ett sådant resultat rutinmässigt.

Phoniro Care: EJ UPPFYLLT. Det saknas rutiner för att säkerställa att en återställning av systemet är möjlig. Det saknas också kompetens hos systemförvaltarna att kravställa och följa upp leverantörens arbete. Det facto att leverantörerna utför rutinmässiga restore tester är självklar bra, men systemförvaltarna bör vara medvetna om detta och utmana leverantörerna att bevisa ett sådant resultat rutinmässigt.

Kontrollfråga 5

Finns det tillräcklig loggning av systemen för att i efterhand få full spårbarhet till vem som har haft tillgång till systemet?

lakttagelse

Procapita: Systemet loggar tid, datum, användare, vad man gjort (till exempel ändringar, journalanteckningar, om man tagit bort en anteckning, eller vilka ärenden man varit inne och titta på) och vart man gjort det. Loggningen ska finnas sedan systemets start. Systemägaren kan se loggar från cirka ett år tillbaka i tiden, men det finns begränsningar på antal poster som visas. Om man vill söka på ett väldigt stort utval så behöver leverantören hjälpa till.

Det är endast systemadmin som har tillgång till att se loggarna. Dock sker ingen monitorering av loggar utan man följer upp enbart vid händelse av en incident.

4 gånger per år görs logguttag av systemet på beställning av förvaltningsjuristen för att kontrollera att ingen obehörig har varit inne i systemet och tittat. Detta är en del av förvaltningens internkontrollarbete. Från och med 2020 kommer loggkontroller att genomföras inom ramen för egenkontroller ute i verksamheterna istället för av förvaltningsjuristen. Detta för att man anser att kvalitén på granskningen blir bättre om granskningen görs närmare verksamheten.

Vid eventuella avvikelser dokumenteras detta i den årliga internkontrollrapporten.

Systemleverantören använder ett ARM system med egen databas för att hantera access loggar till servrarna i driften. Serverloggar kontrolleras maskinellt och databas loggar kontrolleras rutinmässigt.

VKlass: Systemförvaltarna av VKlass kan se de 10 senaste inloggningarna som gjorts av användaren men inte vad användarna har gjort i systemet. Vill man ta reda på aktiviteten i systemet måste man vända sig till leverantören av VKlass.

Phoniro Care: Det finns tre sätt att följa upp användaraktiviteter i Phoniro:

- Åtkomstlogg där kan man se vilken personal som har tittat på vilken brukare, datum, tid och vy.
- Händeslogg/användarkonto, här kan man se vilken person som gjort ändringar på användarkonto, datum och tid.
- Arbetspass, här kan se vem som har skapat ett besök hos brukare, vilka insatser har man gjort, datum och tid

Endast vid misstanke att något har inträffat, eller på begäran av chefen, kontrollerar man loggar. Tas en användare bort ur systemet förlorar man dock spårbarheten för den användaren.

Leverantören loggar aktiviteter som sker på servern och är relaterat till server driften. Loggarna aggregeras och sparas 180 dagar i ett separat system för bland annat uppnå spårbarhet.

Bedömning

Procapita: UPPFYLLT. Det görs stickprov på loggar fyra gånger per år, och slutsatsen dokumenteras i den årliga internkontrollrapporten.

VKlass: EJ UPPFYLLT. Det sker ingen övervakning av aktivitet i systemet, och det går inte heller att på ett smidigt sätt ta fram loggar för att se aktiviteten i systemet om man skulle misstänka en säkerhetsincident. Det saknas även dokumenterade rutiner för incidenthantering inom förvaltningen.

Phoniro Care: DELVIS UPPFYLLT. Det sker loggning i systemet i viss utsträckning. Däremot kontrolleras inte aktiviteter i systemet kontinuerligt och tas en användare bort så förlorar man spårbarheten för den användaren.

Kontrollfråga 6

Är den tekniska säkerheten för systemen på en tillräckligt god nivå för att säkerställa att informationen är skyddad?

lakttagelse

Procapita: Användarens tillgång till systemet sker via en Citrix klient (Citrix Workspace App). Adobe Reader (version 10 eller senare) krävs för utskrifter i Procapita-as-a-Service. Kommunikationen mellan applikationen och servern är krypterad och användarens inloggning sker genom multifactor SAML2 autentisering via Botkyrkas IDP (Nexus Portwise) som driftas av CGI. Systemet i sig har stöd för inloggning via följande metoder, engångslösen via koddosa, e-legitimation (Bank-Id) eller SITHS-kort.

Databasen och backuper är i klartext och lagras inte krypterat vilket heller inte är kravställt i avtalet med Botkyrka kommun.

I det fall ett säkerhetsproblem upptäcks av leverantören, rapporteras det till systemförvaltarna på Botkyrka kommun efter att de har åtgärdats. Senast en rapport om säkerhetsproblem skickades till kommunen var 2019 .

Server driften är skyddat av ett DDOS skydd från internetleverantörer och har inga rapporterade incidenter. Penetrationstester har gjorts mot Procapita, men inte sedan systemet togs i bruk 2013. Vid PwC:s tekniska granskning och intrångstest upptäcktes säkerhetsbrister, där en klassas som hög risk.

Vklass: Vklass kan tillgås via en internetläsare eller mobilapplikation (både för Android och IOS).

Kommunikationen mellan applikationen och servern är SSL krypterad.

Inloggning till både webbapplikationen och mobilapplikationen görs med Botkyrka kommuns federerade inloggning bestående av användarnamn och lösenord. En anledning till att inte multifactor inloggning används, är för att flera användare är lågstadieläro och inte förväntas kunna hantera ett mer avancerat inloggningsförfarande.

Systemet och databasen är delad med Vklass övriga kunder och är inte unik för Botkyrka. Det sker ingen kryptering av databasfält men lösenorden är hashade (SHA265). Regulativa backuper görs av systemet som är definierat av leverantören. Det görs även löpande restore tester i systemet när kunder ber om en återläsning och eftersom systemet är delat med flera kunder anses det som tillräckligt test av funktionen. Botkyrka har inte kravställt en kontroll av detta från leverantören.

Driftlösning är skyddad av brandväggar och har multifactor via DUO app, och Ca 4 personer har tillgång till serverna från leverantören.

Phoniro Care: Phoniro Care är webbgränssnitt för administration av mobiltelefoner, användare för LMHT och e-tillsyn kameror/schemaläggning av e-tillsyn.

Kommunikationen mellan applikationen och servern är SSL krypterad.

Både webbapplikationen och mobilapplikationen som används av Botkyrka kommuns administratörer och användare skyddas med Botkyrka kommuns federerade inloggning bestående av två-faktor autentisering med en koddosa från Portwise. Så fort en applikations stängs ned så måste man identifiera sig igen. För att kontrollera att de mobiltelefoner som används, har de senaste säkerhetsuppdateringarna, är det implementerat ett MDM verktyg (Mobile Device Management). Dock är inte alla telefoner tillräckligt nya och kan inte styras av MDM verktyget, något man hoppas kunna åtgärda inom kort.

Leverantörer gör upprepade penetrationstester mot systemet var 18:e månad för att säkerhetstesta systemet. Resultat- och åtgärdsrapporter tas fram i samband med testerna men delas inte automatiskt med kunderna. Botkyrka kommun har heller inte efterfrågat dessa rapporter.

Bedömning

Enligt de intrångstester PwC gjort har man funnit flera punkter med säkerhetsbrister och potentiella säkerhetshål där en klassats som "HÖG RISK". Intrång- och säkerhetstester är något som ingen av nämndernas förvaltningar krävställer av leverantören och borde göras med jämna mellanrum.

Procapita: EJ UPPFYLLT Systemet använder sig av standardiserade säkerhetsmekanismer för både auktorisation och transport av krypterad data mellan klient och server, databasen och backuperna är dock okrypterade. Senaste en penetrationstest gjordes av systemet var 2013 och bör krav ställas av förvaltaren mer frekvent.

VKlass: DELVIS UPPFYLLT Systemet använder sig av standardiserade säkerhetsmekanismer för både auktorisation och transport av krypterad data mellan klient och server, databasen och backuperna är dock okrypterade.

Phoniro Care: DELVIS UPPFYLLT Systemet använder sig av standardiserade säkerhetsmekanismer för både auktorisation och transport av krypterad data mellan klient och server, databasen och backuperna är dock okrypterade. De mobiltelefoner som inte kan hanteras i MDM verktyget medför en större risk i det fall telefonen faller i orätta händer.

Slutsats

Har vård- och omsorgsnämnden, socialnämnden och utbildningsnämnden säkerställt att informationshanteringen håller en tillräcklig och tillfredsställande nivå för att reducera risker för obehörigt intrång?

Baserat på svaren på kontrollfrågorna ovan från intervjuer och dokumentationsgranskning bedöms Botkyrka kommuns vård- och omsorgsnämnden, socialnämnden och utbildningsnämnden **ej** hålla en tillräcklig och tillfredsställande nivå för att reducera risker för obehörigt intrång.

Det saknas kravställning av att informationen i databaserna skall vara krypterad vilket innebär att systemadministratörer kan ta del av informationen utanför systemets behörighetssystem.






Det saknas kravställning på att genomföra säkerhetstester av systemen med en frekvent intervall. För procapita har det inte genomförts penetrationstester sedan 2013.

Det saknas kravställning om att ha offlinebackuper av informationen i systemen.

Det är möjligt att logga in i Vklass utan krav på stark autentisering.

Rekommendationer

- PwC rekommenderar att kommunens nämnder upprättar ett styrdokument för hur dokument löpande ska revideras och versionshanteras. Det rekommenderas även att de nämnder som saknar styrdokument för informationshantering, upprättar dessa för befintliga system.
- PwC rekommenderar att man säkerställer att kommunens varje användare har genomgått utbildning i systemet och det görs löpande åtminstone 1 gång om året.
- PwC rekommenderar att Botkyrka utbildar systemförvaltarna och upprättar en guide för hur dem rutinmässigt kan ställa krav mot leverantören för att kontrollera att avtalade rutiner uppfylls som t.ex. Backup, restore, spårbarhet och intrångstester.
- PwC rekommenderar att förvaltningen dokumenterar beroendet mellan systemet och stödsystemen, för att uppmärksamma eventuella sårbarheter i behörighets hanteringen, så en säker behörighetskontroll kan säkerställas.

Kontrollmål	Bedömning
<p>Kontrollfråga 1</p> <p>Är befintlig dokumentation gällande rutiner och processer kopplade till informationshanteringen, uppdaterad och löpande reviderad enligt god praxis?</p>	
<p>Kontrollfråga 2</p> <p>Har användarna av systemen en god förståelse om de rådande rutinerna gällande säkerheten av systemen, och säkerställer kommunen att det efterlevs?</p>	
<p>Kontrollfråga 3</p> <p>Har kommunen en process för kontinuerlig behörighetskontroll för att säkerställa rätt behörigheter i systemen?</p>	
<p>Kontrollfråga 4</p> <p>Är möjligheten till återställning av systemen vid en incident kontinuerligt testad och dokumenterad?</p>	
<p>Kontrollfråga 5</p> <p>Finns det tillräcklig loggning av systemen för att i efterhand få full spårbarhet till vem som har haft tillgång till systemet?</p>	

Kontrollfråga 6

Är den tekniska säkerheten för systemen på en tillräckligt god nivå för att säkerställa att informationen är skyddad?



Bilagor

Intervjuer

- Intervju med förvaltningsledare, Socialnämnden, Botkyrka kommun. 2020-04-17 kl 14:00.
- Intervju med systemförvaltare för Procapita, Socialnämnden, Botkyrka kommun. 2020-04-20 kl 13:00.
- Intervju med systemanvändare för Procapita, Socialnämnden, Botkyrka kommun. 2020-04-23 kl 9:00.
- Intervju med leverantör för Procapita, 2020-04-30 kl 11:00.
- Intervju med förvaltningsledare för vård- och omsorgsnämnden, Botkyrka kommun. 2020-04-22 kl 12:00.
- Intervju med systemförvaltare för Phoniro Care, vård- och omsorgsnämnden, Botkyrka kommun. 2020-04-17 kl 15:30.
- Intervju med systemanvändare för Phoniro Care, vård- och omsorgsnämnden, Botkyrka kommun. 2020-04-22 kl 14:00.
- Intervju med leverantör för Phoniro Care, 2020-05-05 kl 10:30.
- Intervju med förvaltningsledare för utbildningsnämnden, Botkyrka kommun. 2020-04-21 kl 14:00.
- Intervju med systemförvaltare för VKlass, utbildningsnämnden, Botkyrka kommun. 2020-04-16 kl 15:00.
- Intervju med systemanvändare för VKlass, utbildningsnämnden, Botkyrka kommun. 2020-04-21 kl 12:00.
- Intervju med leverantör för VKlass, 2020-05-08 kl 13:30.

Dokumentation

Procapita

- Avtal Tieto Procapita 2013
- Generell Guide för Procapita IFO
- Rutin för loggkontroll
- Rättning i Procapita - Guide för hantering av felregistreringar i Procapita IFO
- Behandling av personuppgifter - Uppgifter till förteckning enligt 39§ Personuppgiftslagen
- Riktlinjer för journalföring, informationshantering och åtkomstkontroll av hälso- och vårdjournal
- Socialnämndens dataskyddsrutin
- Socialförvaltningens styrdokument för informationshantering
- Rutin för framtagning av data och loggkontroll inom Socialnämnden
- Personuppgiftsbiträdesavtal - Procapita
- Rapport - Uppföljning av intern kontroll 2019
- Organisation i verksamhetssystemet Procapita gällande Socialförvaltningens vuxenspar

VKlass

- Handlingsplan VKlass
- Systemdokumentation VKlass 2019-04-11




- Avtal Lärarplattform
- Bilaga 2.1. Funktionella krav - Prisbilaga - Utvärdering
- Bilaga 2.2 - Icke-funktionella krav
- Bilaga 2.3 Service Level Agreement
- Personuppgiftsbiträdesavtal
- Dokumenthanteringsplan Utbildningsförvaltningen
- Lösningbeskrivning för Vklass integration mot Extens

Phoniro Care

- E-tillsyn - Krav och förutsättningar - EM014-03 SE
- E-tillsyn - Administration och uppföljning i Phoniro Care -EM008-04 SE
- Checklista LMHT
- LMHT 2 F- Authentication and Resource Request
- Användarmanual Phoniro Care Beskrivning av plattform 16.1.
- Systemkarta inloggning LCMHC
- Skärmdump från intranät - "Viktigt att tänka på gällande informationssäkerhet"
- Skärmdump från intranät - "Användarkonto & behörigheter"
- Skärmdump från intranät - "Informationssäkerhet"
- Policy för informationssäkerhet i Botkyrka kommun

Bedömningsskala

De iakttagelser som diskuterats i denna rapport har bedömts utifrån vilken risk de eventuellt utgör för organisationen. Betygsättningen illustreras med hjälp av trafikljus och ska betraktas som vägledande trots att de är naturligt subjektiva. Det bör noteras att klassificeringen främst fokuserar på graden av behov av ledningens uppmärksamhet och det faktum att en iakttagelse fått ett rött ljus bör inte anses innebära att detta nödvändigtvis utgör en betydande brist.

-  Ett rött ljus ges normalt till iakttagelser som har eller kan ha en betydande inverkan på organisationens finanser och som vi därmed bedömer bör få hög uppmärksamhet. Med avseende på intern kontroll markerar rött ljus en brist som allvarligt påverkar system eller processer som kan leda till stora förluster, ineffektivitet eller andra väsentliga felaktigheter.
-  Gult ljus indikerar ett problem som även om det inte är lika allvarligt som ett rött ljus påverkar eller kan det påverka organisationen på ett sätt som ledningen bör vara medveten om. Med avseende på intern kontroll markerar gult ljus en brist som påverkar system eller processer som kan leda till förluster, ineffektivitet eller andra väsentliga felaktigheter.
-  Ett grönt ljus tilldelas iakttagelser som tidigare har haft ett rött eller gult ljus och som åtgärdats i och med den senaste rapporteringen. Frågor som vi inte anser utgör några problem kan också tilldelas ett grönt ljus om sammanhanget innebär att vi anser att ledningen bör informeras om detta.

2020-06-08

Anders Hägg
Uppdragsledare

Julius Widén
Projektledare

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av Botkyrka kommuns förtroendevalda revisorer enligt de villkor och under de förutsättningar som framgår av projektplan från den 2020-02-05. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.



5

Förvaltningschefen informerar - muntlig information

Beslut

Socialnämnden har tagit del av informationen.

Ärendet

Socialdirektör Marie Lundqvist informerade om aktuella frågor



6

**Samordningsförbundet Botkyrka, Huddinge och Salem (SN
2020:25)**

Det finns inga ärenden att redovisa.



7

Anmälan av delegationsbeslut 2020 (SN 2020:12)

Beslut

Socialnämnden har tagit del av informationen.

Ärende

Dessa delegationsbeslut anmäls till nämnden.

Socialnämndens ordförande

Beslut gällande tillfälligt serveringstillstånd till allmänheten enligt 8 kap 2 § alkohollagen

JK Party Service HB, Botkyrka Golf Restaurang 2020-10-01—10-31



8

Anmälningssärenden 2020 (SN 2020:10)

Beslut

Socialnämnden har tagit del av informationen.

Ärendet

Dessa ärenden anmäls till nämnden:

2020-10-05 Beslut om digitalt sammanträde (SN 2020:270)

I sekretessdelen:

Lex Sarah rapport 1510, 1658, 1670, 1695