Internkontrollrapport per april

Utbildningsnämnd

NORRTÄLJE KOMMUN

Innehåll

Internkontrollrapport

Sammanfattning

Riskpunkter med avvikelser	Antal avvikelser	Planerade åtgärder
Ärenden i funktionsbrevlådor hanteras ej		Inventering av samtliga funktionsbrevlådor Ändrade beställningsrutiner för nya funktionsbrevlådor
IT-system uppfyller inte krav enligt GDPR		Fortsatt kartläggning ”skugg-IT” Fortsatta förhandlingar med leverantör
Obehöriga har åtkomst till personuppgifter i verksamhetssystem		Ny rutin för behörighetsbeställning och uppföljning av behörigheter.
Uppföljning av inventarieregister		Upprätta åtgärdsplan
Bidrag betalas ut på fel grunder		Fastställa rutin för anmälan och mottagande av anmälan för elev med upprepad/längre frånvaro (elev i gymnasieskolan)

Under perioden januari-april har uppföljningar genomförts inom fem av sju kontrollpunkter. Åtgärder har formulerats och följs upp i kommande rapportering.

Effektiva arbetsmetoder och hög kvalitét

Internkontrollområdet syftar till att säkerställa rättssäkerhet och kontinuitet, genom följsamhet till väl fungerande processer och rutiner med ett professionellt bemötande. Det syftar även till att säkerställa följsamhet gentemot kommunens styrdokument, och framställande av korrekta beslutsunderlag.

Kontrollmoment	Frekvens	Metod	Status	Resultat	Åtgärd
Delegationsordningen efterlevs ej					
Kontroll att beslut fattas av rätt person samt att delegationen återrapporteras korrekt	2 ggr per år. Rapporteras vid delår 2 och årsbokslut. Åtgärder vid avvikelse: Information och utbildning av medarbetare.	Stickprov.		Se nedan.	Se nedan. Inga åtgärder.

Resultat:
Stickprovskontroll har genomförts på 11 delegationsbeslut som slumpats fram via en randomiseringstjänst. Urvalet på beslut faller inom det första kvartalet för 2022, d.v.s. januari-mars. Därefter har varje beslut granskats i ärende-hanteringssystemet Platina, om beslutsfattaren stämmer överens med delegationsordningen och att beslutet anmälts till nämnd.
Endast en avvikelse är konstaterad, att ett av besluten ej redovisats nämnd. Detta beror sannolikt på störningar i ärendehanteringssystemet Platina under perioden.

Åtgärd:
Barn- och utbildningskontoret säkerställer att det beslut som ej har anmälts till nämnd anmäls till nästkommande nämndsammanträde samt att kanslienheten säkerställer att funktionen för delegationsrapportering i Platina fungerar enligt kraven.

I övrigt inga åtgärder

Inkommande ärenden i funktionsbrevlådor hanteras ej					
Att inkommande ärenden i funktionsbrevlådor hanteras och registreras i enlighet med hanteringsanvisningarna	1 g per månad.	Stickprov Åtgärd vid avvikelse: Information och utbildning av medarbetare.		Se nedan	Fortsatt inventering Nya beställningsrutiner för nya brevlådor.

Resultat:
Inom utbildningsnämndens ansvarsområde används i dag ett stort antal s.k. "funktionsbrevlådor" /delade brevlådor, d.v.s. "icke personliga" e-postbrevlådor som delas av flera användare och som används i kommunikation både extern och externt för olika specifika ändamål. Barn- och utbildningskontoret ser en risk med att inkommande ärenden i funktionsbrevlådor inte hanteras i enlighet lagens krav på säkerhet, serviceskyldighet och hantering av allmänna handlingar.

Barn- och utbildningskontorets kanslienhet har under perioden börjat med att ta reda på vilka funktionsbrevlådor som finns och om det finns någon formaliserad sammanställning över dessa. Det var inte möjligt att få en avgränsad sammanställning över vilka funktionsbrevlådor som tillhör barn- och utbildningskontorets verksamheter. Granskaren fick därför börja med att försöka avgöra vilka som sannolikt tillhör barn -och utbildningskontorets verksamheter, vilket utgjorde ca 140 st (både BSN och UN). Därefter har stickprov på 15 slumpvis utvalda brevlådor genomförts genom att skicka e-post till dessa brevlådor med följande kontrollfrågor:

- Hanteras och registreras inkommande mail från denna brevlåda?
- Har denna brevlåda daglig bevakning?
- Har denna brevlåda en eller flera ansvariga administratörer?

Under en veckas tid har kontrollanterna mottagit svarsmail från 8 av 15 funktionsbrevlådor (53%). I samtliga mottagna svar så har svarspersonen uppgett ja på de tre kontrollfrågorna, dvs att den aktuella funktionsbrevlådan hanteras och registreras, att den aktuella funktionsbrevlådan har daglig bevakning samt att brevlådan har en eller fler ansvariga administratörer. Samtliga brevlådor har svarat innan 3 dygn och majoriteten av de åtta funktionsbrevlådorna svarade inom 5 timmar.

Resterande 7 (47%) funktionsbrevlådor har vid dags datum ännu inte svarat eller skickat ut svarsmail till kontrollanterna. Därför kan slutsatsen dras att dessa funktionsbrevlådor inte längre används och därmed inte fyller något syfte. Avvikelsen är därmed att 47 % av de kontrollerade brevlådorna inte ger ett svar, något som kan innebära att allmänheten eller interna funktioner inte får svar på sina frågor/ärenden.

Åtgärd:
Barn- och utbildningskontoret ser behovet av en större inventering genomförs genom att identifiera funktionsbrevlådor som inte används och därefter föreslå ansvarig enhet att dessa stängs ner. För att säkerställa att medborgare och interna funktioner får den service de förväntar sig när de vänder sig till en funktionsbrevlåda.

Barn- och utbildningskontoret ser också behov av att införa begränsningar i hur beställning av nya funktionsbrevlådor får ske. Beställning bör bara kunna ske via barn- och utbildningskontorets kanslienhet som då kan säkerställa register över vilka brevlådor som finns, och att det finns en ansvarig administratör som garanterar daglig bevakning av funktionsbrevlådan.

Informationssäkerhet

Kontrollmoment	Frekvens	Metod	Status	Resultat	Åtgärd
IT-system uppfyller inte krav enligt GDPR					
Att datalagring sker i enlighet med GDPR	1 g per år	Totalgranskning av samtliga IT-avtal inom utbildningsnämndens verksamhetsområde. Åtgärder vid avvikelse: Omförhandling av avtal.		Se nedan.	Fortsatt kartläggning av verksamhets-system med fokus på "Skugg-IT" Fortsatta förhandlingar med leverantörer som ej bedöms leva upp till kraven enligt GDPR.

Resultat:
Från och med maj 2022 kommer alla administrativa system hos UN följa GDPR gällande lagring av data. Personuppgiftsbiträdesavtal finns på plats där det behövs och vi genomför regelbundna leverantörsdialoger för att löpande säkerställa att dessa leverantörer möter kraven i GDPR.

Inom utbildningsnämnden finns idag 2 administrativa system UEDB och INDRA som vi anser inte möter kraven i GDPR. Detta för att vi inte har kunnat skriva personuppgiftesbiträdesavtal för att försäkra oss bland annat om vilka underbiträden dessa system använder sig av. Dessa system förvaltas av STORSTHLM. Ingen annan kommun har kunnat skriva personuppgiftsbiträdesavtal kring dessa system och frågan behandlas i nuläget av ett flertal kommuners dataskyddsombud. Dessa system är verksamhetskritiska och det skulle orsaka stor skada om de skulle tas bort.

Två leverantörer av system för pedagogisk verksamhet bedöms inte uppfylla kraven enligt GDPR. Vår data lagras inom EU och kryptering finns på plats men lagringsplatsen ägs av amerikanska bolag och därmed faller under bland annat Cloud Act och fisa 702. Även om risken är minimal kan en situation uppstå där dessa leverantörer skulle vara tvungen att lämna över vår data till amerikanska myndigheter om en så kallade ”executive order” skulle tilldelas dessa leverantörer. Systemen som leverantörerna tillhandahåller bedöms dock verksamhetskritiska, och att sluta använda dem skulle försämra undervisningen markant, bl.a. för elevgrupp med stödbehov.

Det saknas även fullständig information om den s.k. "skugg-IT" som förekommer i verksamheten. Det kan finnas en stor mängd skollicenser (pedagogiska digitala verktyg) som har köps in lokalt på förskolan och skolan som kan bryta mot GDPR. Kunskaper om GDPR och upphandling är allmänt låg på skolnivå vilket kan innebära att pedagogiska digitala verktyg köps in utan hänsyn till vare sig LOU eller GDPR.

Obehöriga har åtkomst till personuppgifter i verksamhetssystem					
Att obehöriga inte har åtkomst till verksamhetssystem, eller fel behörighetsnivå	Kontroller utförs i samband med delårsrapporter och årsbokslut.	Kontroller avser verksamhetssystemen Edlevo, Prorenata och Platina, samt åtkomst till gemensam filkatalog på G:		Se nedan-	Ny rutin för behörighetstilldelning

Resultat:
Ingen särskild kontroll har genomförts under perioden p.g.a. resursbrist (sjukfrånvaro). Däremot har IT-pedagogiska enheten identifierat några brister i rutinerna för behörighetsbeställning som behöver åtgärdas. Det handlar om att system som innehåller känsliga personuppgifter kan ha för stort antal administratörer som dels kan justera sin egen behörighet, dels kan skapa behörigheter till andra utan att det finns någon övergripande kontroll.

Åtgärd:
En åtgärd som planeras att införas inom kort är en s.k. behörighetsbeställning och kontroll i systemet EASIT. Det innebär att den IT-pedagogiska enheten ansvarar för behörighetstilldelning och uppföljning i alla centrala system genom att samtliga användare måste söka behörighet i Easit innan den kan tilldelas.

Spridning av personuppgifter i strid med GDPR och kommunens riktlinjer för webbpublicering					
Att kommunens riktlinjer för webbpublicering följs.	Uppföljning görs 1 g per kvartal och rapporteras i samband med delårsrapporter och årsbokslut			Ej påbörjad	

Internkontrollområdet syftar till att säkerställa att kommunen på ett tillfredsställande sätt hanterar informationssäkerhet på ett relevant sätt. I praktiken bygger detta bland annat på de lagkrav som GDPR (General Data Protection Regulation) ställer, att användare av system har korrekt behörighetsnivå samt att rutiner för IT-konsulter efterlevs i samband med systemutveckling eller systemuppgradering samt att kommunen verkar för rutiner som skyddar invånarnas integritet i data- och informationssystem. I internkontrollområdet inryms även säkerställande av att säkerhetsklassning av särskilda tjänstepersoner är genomförd.

Ekonomi och hushållning av kommunens resurser

Internkontrollområdet syftar till att säkra kommunens tillgångar, en god ekonomisk hushållning och rättvisande redovisning. Det handlar exempelvis om att säkerställa att kommunens resurser används på ett så kostnadseffektivt sätt som möjligt, att fakturor stämmer mot beställning och betalas i tid, att LOU (Lagen om offentlig upphandling) efterlevs. Säkerställande av att kommunen ianspråktar de bidrag och andra intäkter från stat och andra aktörer som kommunen är berättigad till.

Kontrollmoment	Frekvens	Metod	Status	Resultat	Åtgärd
Inventarier (IT-enheter och annan utrustning) avyttras av obehörig eller förkommer					
Att rutiner för uppföljning av inventarieregister finns	Uppföljning sker i samband med delårsrapport och årsbokslut.			Utbildningsnämnden saknar rutiner för uppföljning av inventarieregistret.	En åtgärdsplan tas fram i samråd med kommunstyrelsekontorets redovisningsenhet.
Bidrag betalas ut på fel grunder					
Att det finns rutiner för anmälan av elev med upprepad och/eller längre frånvaro				Se nedan	Fastställa rutin i Skolfyren
Resultat: Enligt skollagens krav ska rektor skyndsamt utreda elev med upprepad eller längre frånvaro. För fristående gymnasieskolor gäller att dessa ska anmäla till hemkommunen om en elev som inte fyllt 20 år utan giltigt skäl är frånvarande i betydande utsträckning. Barn- och utbildningskontoret har en fastställd rutin för anmälan av elever med upprepad eller längre frånvaro för elever i grundskolan. Rutinen finns beskriven i barn- och utbildningskontorets ledningssystem Skolfyren för elever i grundskola och grundsärskola. Däremot saknas rutin i Skolfyren för elever i gymnasie- och gymnasiesärskola.					
Kontroll av bidragsmottagare				Ingen systematisk uppföljning har genomförts under perioden.	