Revisonsskrivelse 2022-09-21

Till: Kommunstyrelsen, Social- och arbetsmarknadsnämnden, Förskolenämnden, Grundskole- och gymnasienämnden

För kännedom: Fullmäktiges presidium

Granskning av stadens hantering av skyddade personuppgifter
EY har på uppdrag av de förtroendevalda revisorerna i Sundbybergs stad granskat om kommunstyrelsen, social- och arbetsmarknadsnämnden, förskolenämnden samt grundskole- och gymnasienämnden har säkerställt att uppgifter som rör skyddade personuppgifter inte röjs till obehöriga samt om stadens rutiner och interna kontroll avseende detta område är ändamålsenliga och tillräckliga. Vår sammantagna bedömning är att kommunstyrelsen och granskade nämnders rutiner och interna kontroll inte är helt ändamålsenliga.

Av granskningen framkommer att styrelse och granskade nämnder i tillräcklig grad inte uppmärksammar respektive sektors hantering av skyddade personuppgifter. Kommunstyrelsen tar inget övergripande samordningsansvar och informationssäkerhetsarbetet, som skyddade personuppgifter i hög grad omfattas av, är eftersatt. Risk- och konsekvensanalyser över hanteringen av skyddade personuppgifter saknas i kommunstyrelsens och granskade nämnders interkontrollplaner.

Granskade sektorer har upprättat verksamhetsspecifika arbetsrutiner för hanteringen av skyddade personuppgifter. Däribland hanteringen av skyddade elever, brukare och anställda i stadens verksamhetssystem, hanteringen av e-post, kommunikation och en riskbedömning över den enskildas hotbild inom skola och socialtjänst. Vår bedömning är att det dock finns anledning att vidta fler och skarpare åtgärder. Då risken att röja skyddade personuppgifter inte bedömts och värderats utifrån risk- och konsekvensanalyser är vår uppfattning att kommunstyrelsen och granskade nämnder inte genomfört relevanta kontrollåtgärder. Det saknas en övergripande strategi eller inriktning för arbetet med skyddade personuppgifter vilket ökar risken för röjning av skyddade personuppgifter i granskade verksamheter.

Granskningen visar att det inte finns antagna rutiner eller riktlinjer för hanteringen av skyddade personuppgifter med undantag för gymnasieskolan. Det anser vi vara en brist. Vi uppmärksammar dock och ser positivt på det utvecklingsarbete som vid granskningens tidpunkt pågår inom både sektorn för lärande och bildning samt välfärd och omsorg vad gäller styrande dokumentation kring hanteringen av skyddade personuppgifter. Att inte kommunstyrelsen har antagit en övergripande riktlinje för stadens hantering av skyddade personuppgifter, däribland medarbetare, bedömer vi vara särskilt allvarligt med tanke på deras övergripande samordningsansvar.

Vidare uppmärksammar vi kompetens och kunskapsspridning som ett särskilt utvecklingsområde. Det saknas kunskap om vilken grundkompetens och fördjupad kompetens som finns om hanteringen av skyddade personuppgifter bland samtliga anställda, det vill säga även de som sällan kommer i kontakt med elever eller brukare med skyddade personuppgifter. Medvetandegrad och kunskapsnivån behöver stärkas genom exempelvis obligatoriska utbildningar och ökad informationsspridning. Detta också varför den mänskliga faktorn genomgående identifierats som den största risken i hanteringen av skyddade personuppgifter.

Slutligen anser vi det vara en brist att det inte går att kategorisera avvikelser som avser skyddade personuppgifter utan manuell hantering. Vi bedömer vidare att det saknas systematik för att åtgärda brister kopplat till hanteringen av skyddade personuppgifter i tillräcklig utsträckning.

Sundbybergs stad

Utifrån granskningens iakttagelser rekommenderar vi kommunstyrelsen, social- och arbetsmarknadsnämnden, förskolenämnden samt grundskole- och gymnasienämnden att:

- Upprätta risk- och konsekvensanalyser avseende hanteringen av skyddade personuppgifter och vid behov låt inkludera i internkontrollplanerna.
- Upprätta och anta styrande dokument för hanteringen av skyddade personuppgifter.
- Överväga att genomföra obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument samt praktisk hantering av vardagssituationer där skyddade personuppgifter förekommer.
- Genomföra penetrationstester och systematiska loggkontroller av IT-system och rutiner för att identifiera sårbarheter och skadekonsekvenser vid intrång samt att obehöriga inte kan få tillgång till skyddade personuppgifter.
- Stärka avvikelsehanteringen och uppföljningen avseende skyddade personuppgifter.

Kommunstyrelsen rekommenderas att:

- Överväga att inom ramen för det övergripande internkontrollansvaret ange risken för röjning av skyddade personuppgifter och inkludera denna i samtliga internkontrollplaner eller i det dagliga arbetet med intern kontroll enligt COSO-modellen.
- Överväga en ”compliancefunktion” med ansvar för strukturerad uppföljning av tillämpning av styrande dokument avseende skyddade personuppgifter.

Granskningen omfattar kommunstyrelsen, social- och arbetsmarknadsnämnden, förskolenämnden samt grundskole- och gymnasienämnden. Det är dock vår bestämda uppfattning att ovanstående rekommendationer är av sådan relevans att samtliga nämnder ska ta dessa i beaktande.

Rapporten överlämnas härmed till kommunstyrelsen, social- och arbetsmarknadsnämnden, förskolenämnden samt grundskole- och gymnasienämnden. Behandlat svar till revisionen önskas senast den 30 november 2022. Rapporten överlämnas även direkt till kommunfullmäktiges presidium för kännedom.

För Sundbybergs stads revisorer

Torbjörn Nylén
Ordförande

HansErik Salomonsson
Vice ordförande

PENNEO

Signaturerna i detta dokument är juridiskt bindande. Dokumentet är signerat genom Penneo™ för säker digital signering. Tecknarnas identitet har lagrats, och visas nedan.

"Med min signatur bekräftar jag innehållet och alla datum i detta dokumentet."

ARVID TORBJÖRN NYLÉN
Undertecknare 1
Serienummer: 19490207xxxx
IP: 193.53.xxx.xxx
2022-09-27 12:40:07 UTC

BankID

HANS ERIK SALOMONSSON
Undertecknare 1
Serienummer: 19540123xxxx
IP: 213.66.xxx.xxx
2022-09-27 17:04:42 UTC

BankID

Penneo dokumentnyckel: Z12LT-5XXJ1-A8EOB-Y5ZJY-QYW1B-CGVZV