

Skrivelse om dataskydd och tydliga brister i hanteringen av personuppgifter

Skrivelse av Jan Jönsson (L), Christofer Fjellner (M) och Jonas Naddebo (C)

Förslag till beslut

Borgarrådsberedningen föreslår att kommunstyrelsen beslutar följande.
Skrivelsen besvaras med hänvisning till vad som sägs i promemorian.

Föredragande borgarrådet Karin Wanngård

Sammanfattning av ärendet

Jan Jönsson (L), Christofer Fjellner (M) och Jonas Naddebo (C) har i en skrivelse till kommunstyrelsen ställt ett antal frågor om stadens hantering av personuppgifter. Frågorna ställs mot bakgrund av att ett fungerande och tillförlitligt dataskydd är avgörande för förtroendet mellan medborgare, företag och förvaltningar. I skrivelsen framförs att när känsliga personuppgifter hanteras på ett sätt som upplevs ovarsamt eller oförutsägbart riskerar människors integritet att skadas, samtidigt som tilliten till viktiga samhällsfunktioner undermineras. Vidare framförs att konsekvenserna av ett dataintrång eller en läcka inte bara är en fråga om juridiska påföljder, utan också en fråga om trygghet och respekt för den personliga integriteten.

Beredning

Ärendet har remitterats till stadsledningskontoret.

Stadsledningskontoret framför att staden arbetar på flera fronter för att säkerställa att personuppgifter hanteras på ett rättssäkert och förutsägbart sätt enligt dataskyddsförordningen (GDPR) och att det finns en systematik i styrning, ansvarsfördelning och uppföljning av dataskyddsarbetet i staden.

Föredragande borgarrådets synpunkter

Systemleverantören Miljödata utsattes för ett dataintrång i augusti och ett stort antal kommuner och andra organisationer drabbades. Stockholms stad har anmält personuppgiftsincidenten till Integritetsskyddsmyndigheten (IMY) och till polisen. En förundersökning om dataintrång pågår. De medarbetare med skyddade

personuppgifter som drabbats har hanterats individuellt och prioriterat. Staden har även tillsatt en extern utredning för att gå till botten med vad vi hade kunnat göra annorlunda och vad vi behöver stärka i fortsättningen.

Tyvärr ser vi att den här typen av kriminalitet blir allt vanligare. Kriminella aktörer utnyttjar sårbarheter i våra system och äventyrar människors säkerhet genom att sprida känsliga uppgifter.

Under den här mandatperioden har vi tagit flera steg för att stärka informationssäkerheten Stadens tillämpningsanvisningar för informationssäkerhet samt rutiner för exempelvis incidenthantering ses över och förbättras varje år.

I budgeten för 2026 lägger stor vikt på informationssäkerhet i staden. Bland annat prioriteras ökad förmåga att förebygga och hantera incidenter. Det finns också direktiv till samtliga nämnder och bolagsstyrelser om att stärka arbetet med informationssäkerhet samt beakta risker och sårbarheter med generativ AI och syntetisk media. Därtill har medel allokaterats till stadsdelsnämnderna om 7,7 mnkr för att stärka det lokala informationssäkerhetsarbetet.

I övrigt hänvisar jag till stadsledningskontorets tjänsteutlåtande.

Stockholm den 19 november 2025

Karin Wanngård

Bilaga

Skrivelse om dataskydd och tydliga brister i hanteringen av personuppgifter, dnr KS 2025/1188–1

Borgarrådsberedningen tillstyrker föredragande borgarrådets förslag.

Särskilt uttalande av borgarråden Christofer Fjellner, Dennis Wedin och Andrea Hedin (alla M) och borgarrådet Jan Jönsson (L) enligt följande.

Efter det allvarliga dataintrånget där känsliga personuppgifter läckt lämnar majoriteten inga tydliga eller tillräckliga svar på våra frågor. Det svar vi fått beskriver främst hur stadens dataskyddsarbete är tänkt att fungera. Det klargör inte vad som faktiskt gått fel, vilka brister som identifierats eller vilka konkreta åtgärder som vidtas för att förhindra att något liknande inträffar igen.

Vi konstaterar att staden undviker att ge ett rakt besked om hur testmiljöer hanteras och om riktiga personuppgifter har använts. Detta är en kärnfråga eftersom just den typen av brister återkommande lett till allvarliga incidenter både i Stockholm och andra kommuner. När svaren uteblir ökar osäkerheten kring om staden verkligen har kontroll över hur våra system är uppbyggda och hur leverantörer får använda stadens data.

Majoriteten ger inte heller någon förklaring till hur oppositionen ska få information i tid vid liknande incidenter framöver. I detta fall informerades vi först efter omfattande medial rapportering. Det är inte acceptabelt. Transparens är en grundläggande del av säkerhetsarbetet och en förutsättning för att hela staden ska kunna ta ansvar.

När det gäller hanteringen av skyddade personuppgifter är svaren alltför generella. Det finns ingen analys av riskerna som uppstod, inga lärdomar och ingen redovisning av vilka förstärkta skyddsåtgärder som införts för de medarbetare som drabbats. Det är särskilt allvarligt eftersom just dessa grupper riskerar allvarliga konsekvenser om deras uppgifter röjs.

Vi saknar dessutom besked om hur staden avser att skärpa kontrollen av sina leverantörer. Intrånget skedde hos en extern aktör och det är därför anmärkningsvärt att inga åtgärder kopplade till kravställning, uppföljning eller säkerhetsrevisioner nämns. När ansvaret är fördelat över flera nämnder och leverantörer krävs ännu tydligare struktur, inte mindre.

Sammantaget kvarstår många obesvarade frågor om huruvida bristerna som ledde till dataintrånget verkligen har tagits på allvar. Medarbetare och invånare måste kunna lita på att deras uppgifter hanteras tryggt och att staden agerar snabbt, öppet och effektivt när säkerheten hotas. Som opposition kommer vi fortsatt att följa frågan noga och kräva de åtgärder som behövs för att stärka förtroendet för stadens dataskyddsarbete.

Kommunstyrelsen

Särskilt uttalande av Christofer Fjellner, Jonas Nilsson och Sophia Granswed Baat (alla M), Jan Jönsson (L) och Jonas Naddebo (C) som är likalydande med Moderaternas och Liberalernas gemensamma särskilda uttalande i borgarrådsberedningen.

Ersättaryttrande av Nike Örbrink (KD) som är likalydande med Moderaternas och Liberalernas gemensamma särskilda uttalande i borgarrådsberedningen.

Ärendet

Jan Jönsson (L), Christofer Fjellner (M) och Jonas Naddebo (C) har lämnat in en skrivelse till kommunstyrelsen om stadens hantering av personuppgifter. I skrivelsen framförs frågor som syftar till en redovisning om stadens arbete med att skydda personuppgifter. Frågorna ställs mot bakgrund av att ett fungerande och tillförlitligt dataskydd är avgörande för förtroendet mellan medborgare, företag och förvaltningar. I skrivelsen framförs att när känsliga personuppgifter hanteras på ett sätt som upplevs ovarsamt eller oförutsägbart riskerar människors integritet att skadas, samtidigt som tilliten till viktiga samhällsfunktioner undermineras. Vidare framförs att konsekvenserna av ett dataintrång eller en läcka inte bara är en fråga om juridiska påföljder, utan också en fråga om trygghet och respekt för den personliga integriteten.

Följande frågor ställs i skrivelsen.

- Hur arbetar staden idag för att säkerställa att personuppgifter hanteras på ett rättssäkert och förutsägbart sätt i enlighet med GDPR?
- Vilka åtgärder vidtas för att säkerställa att staden inte använder testmiljöer med känsliga personuppgifter, och hur kontrolleras detta i praktiken?
- Hur säkerställer majoriteten att oppositionen alltid får insyn i och information om allvarliga brister i dataskyddet?
- Vilka särskilda åtgärder vidtas för att skydda personer med skyddad identitet och individer vars uppgifter rör rehabiliteringsansvar, så att dessa inte riskerar att röjas eller missbrukas?

Remissammanställning

Ärendet har remitterats till stadsledningskontoret.

Stadsledningskontoret

Stadsledningskontorets tjänsteutlåtande daterat den 21 oktober 2025 har i huvudsak följande lydelse.

Staden arbetar på flera fronter för att säkerställa att personuppgifter hanteras på ett rättssäkert och förutsägbart sätt enligt dataskyddsförordningen (nedan GDPR). Detta spänner från styrning, stöttning till uppföljning och stora delar av detta arbete beskrivs övergripande nedan.

Stadens regler för hantering av personuppgifter beskrivs i styrdokument såsom riktlinjer för informationssäkerhet som är beslutade av kommunfullmäktige och omfattar alla nämnder och bolagsstyrelser. Reglerna följer både lagstiftning och etablerade internationella standarder (praxis). De syftar till att staden ska ha ett systematiskt och riskbaserat arbetssätt för dataskydd som håller över tid. Ett område som är särskilt viktigt i styrningen, för att uppnå systematik och hållbarhet i dataskyddsarbetet, är det om roller och ansvar. Att namngivna roller i en verksamhet fått ett formellt ansvar för att genomföra särskilda aktiviteter samt ta ställning till

dataskyddsrisker, är en nyckel i detta avseende. I sammanhanget ska det lyftas att respektive nämnd är en egen myndighet och det innebär också att nämnden är personuppgiftsansvarig för de personuppgifter som nämnden behandlar. Inom staden är därför ansvaret för dataskydd fördelat inom samtliga nämnder och styrelser. I staden finns ett omfattande antal olika system, däribland centrala system och vissa mindre som avser endast en nämnds verksamhetsområde. I styrningen beskrivs även de olika områden som de olika rollerna har ett ansvar för, exempelvis registerförteckning, informationsklassning och konsekvensbedömning.

Utöver styrdokument finns både metodstöd och annat stödmaterial för de aktiviteter som ska genomföras inom ramen för dataskyddsarbetet. Det finns även ett antal e-utbildningar om dataskydd som samtliga förvaltningar/bolag kan använda. En av dessa är obligatorisk för stadens alla medarbetare och genomförandet följs upp genom certifieringar och statistikfunktioner.

En viktig del i att uppnå ett systematiskt och hållbart dataskyddarbete över tid är uppföljning. Enligt dataskyddsförordningen ska respektive personuppgiftsansvarig ha ett förordnat dataskyddsombud som ansvarar för att övervaka efterlevnaden av dataskyddsförordningen bland annat genom uppföljning samt råd och stöd. Nämnden och styrelsen har, i egenskap av personuppgiftsansvarig, ett ansvar att följa upp eventuella dataskyddsrisker inom sitt ansvarsområde. I dataskyddsombudets årsrapport, som bifogas som en bilaga till verksamhetsberättelsen, informeras nämnden/styrelsen om nuläge och identifierade dataskyddsrisker. I rapporten lämnas också rekommendationer för vidare utveckling eller åtgärder under kommande år, i syfte att uppfylla dataskyddsförordningen.

Med ”testmiljö” menas ofta en miljö där man genom simulation ska upptäcka defekter i en programvara. Stadens kravställning runt testdata framgår av både styrdokument och metodstöd. De följer principerna i dataskyddsförordningen. I stadens regelverk framgår även att en särskild riskanalys avseende personuppgifterna (konsekvensbedömning) ska genomföras innan behandlingen, exempelvis innan testning.

Staden har idag en rutin där personer som har fått skyddade personuppgifter från Skatteverket ska anmäla detta till arbetsgivaren. En markering i stadens löneadministrativa system om skyddade personuppgifter görs. Ett utvecklingsarbete att integrera Skatteverkets markering om beslut om skyddade personuppgifter pågår, och det finns i övergångsperioden en särskild rutin för hämtning av uppgifterna.

För personer med skyddade personuppgifter genomförs individuella riskbedömningar hos respektive nämnd och bolag och en handlingsplan för skyddsåtgärder upprättas utifrån de individuella förutsättningarna som finns. Hantering av uppgifter som rör arbetslivsinriktad rehabilitering styrs av stadens rehabiliteringsprocess där det finns angett hur uppgifterna ska hanteras.