

Rapport dataskyddsombudets granskning 2025

Miljöförvaltningen

Upprättad av
Martin Axelsson
Dataskyddsombud

Stadskontoret, Juridiska enheten
martin.axelsson2@malmo.se

Innehåll

Rapport dataskyddsombudets granskning 2025.....	1
1. Inledning	3
1.1. Bakgrund och mottagare.....	3
1.2. Innehåll och syfte.....	3
2. Väsentligheter från det gångna året.....	4
2.1. Internt.....	4
2.1.1. Stadsövergripande process för hantering av personuppgiftsincidenter närmare.....	4
2.1.2. Kamerabevakningsrådet	4
2.1.3. Ökad samordning kring frågor av betydelse för stadens informationssäkerhet, dataskydd och IT-säkerhet.....	4
2.1.4. Ny modell för hantering av interna och externa biträdesrelationer.....	5
2.2. Externt – väsentligheter under året.....	5
2.2.1. Ändringar i Kamerabevakningslagen har trätt i kraft.....	5
2.2.2. Förändringar i GDPR	6
2.2.3. Tillsynsåret.....	6
3. Periodisk granskning	7
3.1. Dataskyddsorganisationen.....	7
3.2. Behandlingsregister.....	7
3.3. Utbildning.....	8
3.4. Registrerades rättigheter.....	8
3.5. Konsekvensbedömning	8
3.6. Pub-avtal och leverantörsuppföljning.....	9
3.7. Personuppgiftsincidenter.....	9
4. Övrig granskning.....	10
5. Rekommendationer till personuppgiftsansvarig.....	10

1. Inledning

1.1. Bakgrund och mottagare

Enligt Dataskyddsförordningen artikel 38.3, ska dataskyddsombudet rapportera till en personuppgiftsansvarigs högsta förvaltningsnivå. I Malmö stad är de enskilda nämnderna ansvariga för den behandling av personuppgifter som sker inom deras verksamhetsområde, och således är det till nämndernas högsta förvaltningsnivå sådan rapportering ska riktas, vilket tolkas som förvaltningens ledning.

1.2. Innehåll och syfte

Rapporten består av denna inledning, en redogörelse för väsentliga interna och externa händelser och utveckling under det gångna året och därefter en genomgång av den periodiska granskning som genomförs av dataskyddsombudet varje år. Det är denna periodiska granskning som utgör den huvudsakliga rapporteringen om personuppgiftsansvariges egen verksamhet. Granskningen berör sju olika områden – Dataskyddsorganisation, Behandlingsregistret, Utbildning, Registrerades rättigheter, Konsekvensbedömning, Personuppgiftsbiträdesavtal och leverantörsuppföljning samt Personuppgiftsincidenter. Till detta redogörs för eventuella övriga granskningar som angår förvaltningen. Rapporten avslutas med rekommendationer till den personuppgiftsansvarige.

Syftet med rapporten är att personuppgiftsansvarig ska få en lägesbild över den egna förvaltningens dataskyddsarbete, kunna följa utvecklingen inom detsamma och ha möjlighet att identifiera såväl positiva som negativa tendenser. Syftet är också att informera personuppgiftsansvarig om såväl stadens övergripande arbete med dessa frågor, som områdets utveckling i omvärlden, däribland tillsynsmyndighetens arbete.

2. Väsentligheter från det gångna året

2.1. Internt

2.1.1. Stadsövergripande process för hantering av personuppgiftsincidenter närmare

I och med att det nya ITSM-systemet kommer på plats, kommer det skapas förutsättningar för att i detta bygga en övergripande hantering av personuppgiftsincidenter i staden. I dagsläget hanteras personuppgiftsincidenter enligt lokala processer på de enskilda förvaltningarna. En central hantering av detta kommer ge tydligare tillvägagångssätt för medarbetarna som rapporterar, mer enhetlig bedömning av incidenter och för centrala funktioner tillgängliggöra det kunskapsunderlag som rapporterade incidenter innebär.

2.1.2. Kamerabevakningsrådet

Under året har centrala rådet för kamerabevakning bildats. Syftet är, mot bakgrund av förändringar i lagstiftningen, att stödja stadens verksamheter med bedömningar om huruvida en planerad kamerabevakning är laglig, samt att tillhandahålla verktyg och stöd för att få en gemensam och rättssäker process i staden kring frågor om kamerabevakning.

2.1.3. Ökad samordning kring frågor av betydelse för stadens informationssäkerhet, dataskydd och IT-säkerhet

En ny struktur för samordning av frågor som har betydelse för stadens informationssäkerhet, dataskydd och IT-säkerhet har etablerats. Denna består av en samordnande nivå bestående av centrala funktioner för dataskydd, informationssäkerhet och IT-säkerhet, samt en inriktande nivå bestående av

verksamhetsansvariga chefer för dessa funktioner. Syftet med strukturen är att säkerställa att frågor som berör stadens informationssäkerhet, dataskydd och IT-säkerhet fångas upp och hanteras på ett lämpligt och effektivt sätt.

2.1.4. Ny modell för hantering av interna och externa biträdesrelationer

Ett arbete har pågått under året med att utreda hur en mer effektiv reglering av personuppgiftsbehandlingar som involverar flera nämnder och extern leverantör, kan införas i staden. I dagsläget hanteras ofta sådana situationer genom att varje nämnd tecknar separata personuppgiftsbiträdesavtal med leverantörer, även för leveranser som avser hela staden. Denna ordning har i vissa delar visat sig opraktiskt och otillfredsställande, och arbetet har fokuserat på att hitta och pröva modeller för att förenkla och effektivisera både de interna ansvarig-biträde-relationerna och förhållandet till externa leverantörer. Ett färdigt förslag beräknas till början av nästa år.

2.2. Externt – väsentligheter under året

2.2.1. Ändringar i Kamerabevakningslagen har trätt i kraft

Ändringar i kamerabevakningslagen trädde i kraft i april i år. De nya reglerna innebär att en personuppgiftsansvarig som vill bedriva kamerabevakning nu inte behöver söka tillstånd för detta, men måste bland annat dokumentera en intresseavvägning som visar om den planerade kamerabevakningen är rimlig och proportionerligt i förhållande till integritetsintresset på platsen.

2.2.2. Förändringar i GDPR

Året har präglats av diskussion kring behov av att förenkla Dataskyddsförordningen för att underlätta efterlevnad, men också för att underlätta utveckling inom AI. Förändringarna rör bland annat registrerades rättigheter, rapportering av personuppgiftsincidenter och hur konsekvensbedömningar upprättas, men också själv definitionen av begreppet personuppgift.

2.2.3. Tillsynsåret

Tillsynsmyndighetens arbete har inte visat någon tydlig tendens i år, utan man fortsätter av allt att döma att arbeta brett. Något som kan noteras bland tillsynsärenden är att de som initieras på grund av incidentanmälningar eller klagomål från enskilda har blivit fler, vilket sannolikt har att göra med diskussionen kring tillsynsmyndighetens generella hantering av klagomål, och huruvida denna är rättssäker nog. Bland intressanta ärenden hos IMY kan nämnas en tillsyn riktad mot Diskrimineringsombudsmannen, där IMY utfärdade en sanktionsavgift på 100 000 kronor efter att myndigheten bedömde att DO inte vidtagit tillräckligt effektiva säkerhetsåtgärder i samband med insamling på sin hemsida av tips och klagomål rörande diskriminering. Ett annat ärende rör Region Uppsala, där IMY tilldelade sjukhusstyrelsen en reprimand efter att ha konstaterat att patientuppgifter rörande hälsa hanteras i Outlook. Båda dessa ärenden inleddes efter att respektive personuppgiftsansvarig anmält personuppgiftsincidenter till IMY.

3. Periodisk granskning

3.1. Dataskyddsorganisationen

Personuppgiftsansvarigs dataskyddsorganisation består av 4 personer, med en dataskyddssamordnare som för sitt dataskyddssamordnarskap har 33% av en heltidstjänst. Utöver dataskyddssamordnare ingår i dataskyddsorganisation representanter för arkiv, registrering och systemförvaltning.

Det finns ett strukturerat arbetssätt som utgår från verksamhetsprocesserna beskrivna i arkivredovisningen, där enhetscheferna är kontaktpersoner för sina respektive processer i arkivredovisningen och registerförteckningen, och dessa ansvarar för att meddela förändringar i informationshanteringen i verksamheten.

Arbetsgruppen som utgör dataskyddsorganisationen träffas veckovis. Det rapporteras att dataskydd inte är detta forums primära syfte, men att dataskydd utgör en integrerad del av de styr- och ledningsfrågor som diskuteras i forumet.

Rapportering finns etablerat på förvaltningen, med årlig rapportering till förvaltningsledning och nämnd.

3.2. Behandlingsregister

Personuppgiftsansvarig har 84 behandlingar registrerade i sitt artikel 30-register. Det finns en tät samordning mellan arkivprocesserna och registerförteckningen och uppdatering av registret sker löpande i samband med uppdatering av arkivredovisning. Som nämns under 3.1. så finns också kontaktpersoner för respektive process ute i verksamheterna, vilket bör i hög grad säkerställa att registerförteckningen speglar de faktiska verksamhetsprocesserna. Miljöförvaltningens arbete med registerförteckningen ger därmed intryck av att vara i hög grad välfungerande och är sannolikt det mest välutvecklade i staden.

3.3. Utbildning

Förvaltningens medarbetare har under det gångna året haft tillgång till den stadsövergripande utbildningen i dataskydd. Det rapporteras att 62% av medarbetarna har slutfört denna, vilket är en hög siffra. Denna utbildning är nu avslutad, men kommer ersättas av en likvärdig utbildning i Malmö lär som personuppgiftsansvarig rekommenderas att ansluta sig till. Utöver detta rapporteras att det genomförts utbildningsinsatser med fokus på personuppgiftsincidenter och lokal hantering under året. Det uppskattas att över 80% av medarbetarna har deltagit i denna. Det framstår därmed som att personuppgiftsansvarig arbetar aktivt och framgångsrikt med utbildningsinsatser kring dataskydd.

3.4. Registrerades rättigheter

Hanteringen kring registrerades rättigheter sköts huvudsakligen genom Malmö stads e-tjänst för detta ändamål. Utifrån vad undertecknad har inhämtat vid tidigare tillfällen så fungerar denna tillfredsställande.

Aktiviteten inom området är som i resten av staden mycket låg. Under 2024 inkom en begäran enligt registrerades rättigheter, avseende registerutdrag. Siffran för första halvan av 2025 är en begäran, också avseende registerutdrag.

Staden och nämnden har fungerande process på plats för att motta och efterkomma registrerades rättigheter. Det saknas skäl att rekommendera några åtgärder.

3.5. Konsekvensbedömning

Personuppgiftsansvarig använder den stadsövergripande mallen för att bedöma om en behandling innebär hög risk för den registrerade, och för att i förekommande fall genomföra konsekvensbedömning.

Det har genomförts endast en konsekvensbedömning på förvaltningen, detta 2024. Utifrån vad som tidigare och i andra sammanhang inhämtats så görs dock bedömningen att detta är tillräckligt givet den riskbild som verksamheten har, och det har inte framkommit något som tyder på att denna bedömning skulle vara oriktig. Det saknas alltså skäl att rekommendera några åtgärder här.

3.6. Pub-avtal och leverantörsuppföljning

Personuppgiftsansvarig har en rutin för att säkerställa tecknande av Pub-avtal, som ingår i den allmänna avtalsrutinen, och den stadsövergripande mallen för pub-avtal används. Det har aldrig skett att en leverantörs förslag till pub-avtal har accepterats.

Ifråga om överföring av personuppgifter till tredje land så rapporteras att detta huvudsakligen sker genom de stadsövergripande tjänsterna i Office365. Personuppgiftsansvarig har rutiner och riktlinjer för vilken information som får hanteras i dessa tjänster.

Gällande uppföljning av dataskyddsfrågor gentemot leverantör så görs inte detta systematiskt. Det finns ett arbetssätt på plats där systemägare och leverantör stämmer av, och detta rapporteras på sikt kunna inkludera dataskyddsfrågor. Förvaltningen har också deltagit i det stadsövergripande arbetet med leverantörsuppföljning.

3.7. Personuppgiftsincidenter

Personuppgiftsansvarig har en välutvecklad hantering av personuppgiftsincidenter. Verksamheten rapporterar incidenter i formulär framtaget i Forms. Detta hamnar i en funktionsbrevlåda på dataskyddsamordnarens enhet. Därefter hanteras incidenten av dataskyddsamordnaren eller dennas ersättare vid frånvaro. Dataskyddsamordnaren avgör inledningsvis om det är en incident som kan behöva rapporteras till IMY, och i sådana fall bokas skyndsamt möte upp med ansvarig informationsägare där vi tillsammans fyller i förvaltningens mall för att dokumentera

personuppgiftsincidenter och avgör om det är något som behöver rapporteras till IMY. Incidenter rapporteras till IMY när det inte kan utesluta att det finns en risk för den registrerades integritet, och denna bedömning utgår från en riskmatris. Incidentrapporter ger i regel upphov till en åtgärdsplan som informationsägaren implementerar och denna följs upp av dataskyddssamordnare. Rapporten förvaras i förvaltningens diarium tillsammans med eventuell dokumentation om att anmäla till IMY.

Under 2024 rapporterades 2 incidenter, av vilka ingen anmäldes till IMY. Första halvan av 2025 rapporterades 3, varav en anmäldes till IMY. Siffran framstår som förhållandevis låg, men det är av naturliga skäl svårt att bedöma hur stort ett mörkertal kan vara. Personuppgiftsansvarig rekommenderas att fortsätta arbetet med informationsinsatser kring personuppgiftsincidenter.

4. Övrig granskning

Dataskyddsombudet har granskat huruvida miljönämnden bedriver någon kamerabevakning i enlighet med kamerabevakningslagen och huruvida nämnden i så fall har upprättat en förteckning över denna i enlighet § 10 kamerabevakningslagen.

Nämnden bedriver enligt vad som inhämtats ingen sådan kamerabevakning i dagsläget.

5. Rekommendationer till personuppgiftsansvarig

- Anslut förvaltningen till den kommande stadsövergripande dataskyddskursen i Malmö Lär
- Fortsätt arbeta med informationsinsatser om personuppgiftsincidenter