

Rapport dataskyddsombudets granskning 2023

Miljöförvaltningen

Upprättad 2023-12-21 av

Martin Axelsson
Dataskyddsombud

Stadskontoret, Juridiska enheten
martin.axelsson2@malmo.se

Innehåll

Rapport dataskyddsombudets granskning 2023.....	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. Ny tjänst dataskyddsspecialist	4
2.1.2. Rapportering till högsta förvaltningsnivå	4
2.1.3. Ny metod för tröskelanalys och konsekvensbedömning.....	4
2.1.4. Övrigt pågående arbete	5
2.2. Externt	5
2.2.1. Väsentligheter under året.....	5
2.2.2. Tillsynsåret	6
3. Periodisk granskning	6
3.1. Dataskyddsorganisationen	6
3.2. Behandlingsregister	7
3.3. Utbildning.....	7
3.4. Registrerades rättigheter	8
3.5. Konsekvensbedömning.....	8
3.6. Pub-avtal och leverantörsuppföljning.....	8
3.7. Personuppgiftsincidenter	9
4. Övrig granskning.....	9
5. Rekommendationer till personuppgiftsansvarig	9

1. Inledning

1.1. Bakgrund och mottagare

Enligt Dataskyddsförordningen artikel 38.3, ska dataskyddsbudet 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 hädanefter genomförs av dataskyddsbudet 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. Ny tjänst dataskyddsspecialist

Under året har det tillkommit en ny roll på stadskontoret – stadens dataskyddsspecialist har ett stadsövergripande, strategiskt uppdrag att driva dataskyddsarbetet framåt i staden som helhet. Tidigare fanns en organisatorisk otydlighet kring vilken roll som bör axla huvudansvaret för det framtidsytande och strategiska arbetet med stadsövergripande dataskyddsfrågor. I praktiken landade dessa frågor ofta hos dataskyddsombudet, vilket kunde ge upphov till frågeställningar kring Dataskyddsombudets roll som oberoende. I och med att dessa frågor nu har en tydlig och naturlig hemvist skapas förutsättningar för ett mer effektivt arbetssätt centralt i denna del.

2.1.2. Rapportering till högsta förvaltningsnivå

Arbete pågår med att etablera rapportering från Dataskyddsombudet till samtliga personuppgiftsansvariga, där denna rapport är en del. Tidigare har ingen formaliserad eller regelbunden rapportering av detta slag skett, vilket får betraktas som en brist vi i och med detta försöker avhjälpa.

2.1.3. Ny metod för tröskelanalys och konsekvensbedömning

Under året har ett nytt mall- och metodstöd för tröskelanalys och konsekvensbedömning arbetats fram genom samarbete mellan stadens dataskyddsjurist, Dataskyddsombud, informationssäkerhetssamordnare samt Serviceförvaltningen dataskyddssamordnare. Detta är nu tillgängligt för alla, och förväntas leda till att verksamheten i högre grad genomför konsekvensbedömningar.

2.1.4. Övrigt pågående arbete

- Arbete pågår med att kartlägga de olika incidentprocessflödena i staden, där hanteringen av personuppgiftsincidenter är ett. Ambitionen är att skapa en mer enhetlig rapportering av incidenter i staden, undvika dubbelrapportering och utnyttja synergieffekter där så är möjligt.
- En utredning har initierats av stadens informationssäkerhetssamordnare, där en extern konsult har upphandlats för att utreda hur en laglig och effektiv informationsförvaltningsmodell kan se ut i staden. Detta omfattar också personuppgiftsansvaret.
- Några förvaltningar har påbörjat ett arbete med att omarbeta sina registerförteckningar. Utgångspunkten ska vara verksamhetens processer och registerförteckningen ska beskriva den behandling av personuppgifter som sker däri. Ambitionen är att detta nya sätt att upprätta registerförteckningen ska tjäna som modell för resten av staden.

2.2. Externt

2.2.1. Väsentligheter under året

Den enskilt största nyheten under året torde vara adekvansbeslutet som återigen gör det möjligt att på ett praktiskt sätt föra över personuppgifter till USA. Det finns dock frågetecken kring hur pass stabilt rättsläget är, särskilt med beaktande av Max Schrems uttalande att man avser utmana beslutet rättsligt, i likhet med vad man gjort med tidigare. Om verksamheter i staden vill använda sig av nya tjänster eller leverantörer som skulle innebära överföring av personuppgifter till USA, så är risken för ett snabbt förändrat rättsläge något man bör beakta.

2.2.2. Tillsynsåret

Året har inte bjudit på något tydligt tema i fråga om tillsynsmyndighetens aktiviteter, utan man har av allt att döma fortsatt att arbeta förhållandevis brett gentemot både privat och offentlig sektor.

Värt att notera för stadens del är ett visst fokus på kamerabevakning som troligen kan förväntas fortsätta, då det utgör en förhållandevis gripbar och enkel sak att rikta ett tillsynsärende mot. Även ett ärende mot Östersunds kommun är värt att ta notis om – IMY utdelade här en sanktionsavgift för underlåtenhet att genomföra konsekvensbedömning innan den digitala plattformen Google Workspace infördes på skolor i kommunen. Ärendet understryker vikten av att stadens verksamheter i högre grad genomför konsekvensbedömningar.

En sannolik utveckling framöver kommer vara att tillsynsmyndigheten tvingas lägga mer resurser på att vidta åtgärder i samband med enskildas klagomål, då Högsta förvaltningsdomstolen har beslutat att tillsynsmyndighetens beslut är överklagbara. Tidigare gällde resonemanget att sådana beslut inte är överklagbara eftersom de inte påverkar en enskild i sådan omfattning som krävs enligt förvaltningslagen, för att beslutet ska vara överklagbart. Detta kan förväntas leda till IMY tvingas prioritera annorlunda framöver.

Av direkt intresse för staden kan nämnas den tillsyn som riktades mot ASF, angående Dataskyddsombudets roll- och resursfördelning. Denna omfattade ett stort antal offentliga verksamheter i Sverige, och var ett samarbete mellan ett flertal tillsynsmyndigheter i EU, initierat av Europeiska Dataskyddsstyrelsen. Upplägget var ett enkelt frågebatteri som besvarades skriftligt. Tillsynen har inte lett till några åtgärder, vare sig från IMY eller internt i Malmö stad.

3. Periodisk granskning

3.1. Dataskyddsorganisationen

Frågan om vilka roller som ingår i förvaltningens dataskyddsorganisation och hur omfattande den är saknar ett enkelt svar. Arbetet drivs i huvudsak av dataskyddssamordnare i samarbete med huvudregistrator/arkivarie. Andra roller som är intressenter i förvaltningens dataskyddsarbete är informationssäkerhetssamordnare, jurist och representanter för

informationsägare. Det finns inget formellt nätverk, men efter de olika rollerna arbetar på samma enhet så behövs det inte heller.

Miljöförvaltningen är i och för sig en av stadens mindre förvaltningar, men personuppgiftsansvarig bör ändå överväga om nuvarande dataskyddsorganisation är tillräcklig för att hålla effektiv uppsikt över verksamheten med avseende på dataskydd. På ett flertal andra förvaltningar finns minst en kontaktperson för dataskydd per avdelning. Personuppgiftsansvarig bör överväga om något liknande är lämpligt på miljöförvaltningen.

Vad gäller rapportering så finns beslut från 2023 att dataskyddssamordnare ska rapportera till såväl nämnd som förvaltningsledning. Det är positivt att detta har etablerats.

3.2. Behandlingsregister

Det finns 84 behandlingar registrerade i förvaltningens behandlingsregister. Det noteras att utgångspunkten vid registerförteckningens upprättande har varit verksamhetens processer så som de finns beskrivna i förvaltningens arkivredovisning. Detta är positivt eftersom det innebär att det finns ett principiellt och enhetligt tillvägagångssätt att beskriva och avgränsa en behandling, vilket underlättar ordning och reda i registret.

Senast en översyn gjordes av registret var i samband med migreringen till Ifacts 2022 och en större genomlysning pågår under detta året och nästa. Endast en (1) ny behandlingsaktivitet har anmälts detta året.

3.3. Utbildning

Det har genomförts utbildningar inom området på APT hos alla avdelningar på förvaltningen under 2023, men det finns inga detaljerade uppgifter kring närvaro eller om deltagarna har tillgodogjort sig innehållet. Utöver detta ges grundläggande information om dataskydd i introduktionsutbildningen. Därtill har en grundläggande utbildning i dataskydd för kommuner upphandlats av kommunstyrelsen. Denna är tillgänglig för miljöförvaltningen och samtliga medarbetare som i sin

tjänsteutövning behandlar personuppgifter förväntas genomgå denna.

Personuppgiftsansvarig bör överväga om det finns behov av mer målgruppsanpassade utbildningar.

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.

Under 2022 inkom tre begäran enligt registrerades rättigheter, samtliga avseende registerutdrag. Motsvarande siffra för första halvan 2023 är noll (0)

Hur många begäran som kan förväntas beror i hög grad på vilken verksamhet som bedrivs och vilka de registrerade är. Antalet inkomna begäran ger inte skäl att överväga några åtgärder.

3.5. Konsekvensbedömning

Det har inte genomförts några konsekvensbedömningar på förvaltningen. Det är oklart om detta beror på att det helt enkelt inte finns några behandlingsaktiviteter där detta behövs. Det rapporteras att förvaltningen använder den stadsövergripande mallen för att bedöma om en behandling innebär hög risk för den registrerade, men denna har tillkommit nyligen, och det är därmed inte orimligt att det bland redan befintliga behandlingar finns sådana som egentligen skulle konsekvensbedömas. Personuppgiftsansvarig bör undersöka hur detta förhåller sig.

3.6. Pub-avtal och leverantörsuppföljning

Förvaltningen har en egen rutin för Pub-avtal. Innehållet i denna har inte granskats, men det framstår som positivt att den finns, i det att en särskild rutin ger bättre möjligheter att övervaka och motverka risker som är specifika för miljöförvaltningens verksamhet. Vidare rapporteras att det under 2023 genomförts en genomlysning av PUB-

avtal har avtal som inte är i enlighet med de centrala mallarna identifierats och process har startats för att uppdatera avtal utifrån Stadens centrala/SKR:s mall. Allt detta är positivt och ger intryck av att det råder ordning och reda inom detta område. I fråga om leverantörsuppföljning så finns inget systematiskt arbete.

3.7. Personuppgiftsincidenter

Verksamheten rapporterar personuppgiftsincidenter genom ett Forms-formulär som medarbetare kommer åt via Komin. Detta framstår som en enkel och praktisk lösning givet att inget tillfredsställande stadsövergripande rapporteringsverktyg finns.

I fråga om antalet rapporterade incidenter var dessa två (2) under 2022, varav 0 anmäldes till IMY. Under 2023 till och med juni har det rapporterats en (1) incident, och denna enda har också anmälts till IMY.

Det finns sannolikt en kraftig underrapportering.

Personuppgiftsansvarig bör vidta åtgärder för att öka mängden rapporterade incidenter.

4. Övrig granskning

Ingen övrig granskning avseende miljöförvaltningen har skett under året.

5. Rekommendationer till personuppgiftsansvarig

- Överväg om nuvarande dataskyddsorganisation är tillräckligt utbyggd för att hålla effektiv uppsikt.
- Tillse att samtliga medarbetare som behandlar personuppgifter genomgår den av kommunstyrelsen upphandlade grundutbildningen, och överväg behovet av målgruppsanpassade utbildningar inom dataskydd.
- Vidta åtgärder för att öka antalet konsekvensbedömningar eller inventera behandlingar där en konsekvensbedömning behövs.

- Överväg vilka möjligheter som finns i frågan om leverantörsuppföljning. Uppföljning gentemot leverantör är eftersatt i hela staden, men är ofta ett besvärligt och resurskrävande arbete. Personuppgiftsansvarig bör överväga vilka behov som finns och vilka resurser som kan avsättas för ett systematiskt arbete, liksom vilka riskerna är om detta arbete brister.
- Vidta åtgärder för att öka mängden rapporterade personuppgiftsincidenter. Detta kan tillgodoses åtminstone delvis av adekvata och kontinuerliga utbildningsinsatser.