Stockholms stad

Dataskyddsombudets årsrapport

År 2025

Hägersten-Älvsjö stadsdelsnämnd

Dataskyddsombudets årsrapport
December 2025

Dnr: HÄ 2025/899
Utgivningsdatum: 2025-12-19
Kontaktperson: Christian Sandell

Sammanfattning

GDPR, eller dataskyddsförordningen, syftar till att skydda individers grundläggande rättigheter och friheter, med särskilt fokus på rätten till skydd av personuppgifter. I Stockholms stad är varje nämnd och styrelse ansvarig för personuppgiftsbehandlingar som sker i den egna verksamheten. Som dataskyddsombud är uppdraget att oberoende granska verksamhetens efterlevnad av dataskyddsförordningen. Allt operativt dataskyddsarbete ansvarar dock stadsdelsförvaltningen för.

I denna rapport redovisas årets granskning av Hägersten Älvsjö Stadsdelsnämnds dataskyddsarbete samt lämnas rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

Den enskilt största händelsen som inträffade år 2025 var Miljödataincidenten där även personuppgifter gällande samtliga anställda och även tidigare anställda vid stadsdelsförvaltningen togs över av en utomstående part och hamnade på det så kallade Dark Net. Då utredningarna om vad som faktiskt hände ännu inte är avslutade så finns det anledning att avvakta med att ta ställning om även stadsdelsförvaltningen brustit i sitt agerande (eller brist på agerande) när det gäller skyddet av de anställdas personuppgifter. Oberoende av ansvarsfrågan så kan Miljödataincidenten trots allt visa på svagheter i organisationen av dataskyddsarbetet inom staden och även inom stadsdelsförvaltningen.

De tre största riskerna enligt dataskyddsombudets bedömning

Den första av de tre största riskerna är att det saknas ett organiserat dataskyddsarbete inom stadsdelsförvaltningen som kan hålla ihop alla dataskyddsfrågor som måste hanteras inom en verksamhet för att kunna leva upp till alla de krav som dataskyddsförordningen GDPR kräver. Miljödataincidenten visar på att vi sannolikt inte har haft den kontroll som vi borde haft över de personuppgifter som rör alla våra anställda och tidigare anställda.

Den andra risken är att vi inte har kontroll över den information om personuppgiftsbehandlingar som ska finnas tillgänglig för våra brukare och för våra anställda. Att informera om de personuppgiftsbehandlingar som sker inom verksamheten är en grundläggande förutsättning för att över huvud taget få behandla personuppgifter i många situationer. Även här kan Miljödataincidenten ge oss en tydlig påminnelse då vi såvitt kunnat bedömas inte har lämnat information till våra anställda att deras uppgifter, även integritetskänsliga sådana (hemadresser och skyddade uppgifter) skulle användas i utvecklingsarbetet vid framtagning av nya tjänster inom staden. Stadsdelsförvaltningen behöver ta kontrollen över denna information.

Även den tredje risken rör frågor som är högst aktuella med anledning av Miljödataincidenten nämligen vem som ansvarar för personuppgiftsbehandling som blir aktuell när vi inom staden utvecklar nya tjänster och hur vi kan försäkra oss om att ”våra” uppgifter skyddas även då utveckling sker inom annan förvaltning inom staden. Är det vi som personuppgiftsansvariga så har vi ett ansvar för att ”våra” uppgifter skyddas även när behandlingar sker utanför vår verksamhet. Vi måste även ha kontrollen över ”vår” information när den behandlas i centrala system men för vår räkning. Vi har idag ingen organisation som klarar av att följa upp denna viktiga fråga.

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Personuppgiftsansvarigs Ansvarsskyldighet		Förvaltningen måste ges i uppdrag att organisera ett löpande dataskyddsarbete som klarar av att hantera de krav som GDPR ställer på en personuppgiftsansvarig. Detta kräver bland annat att en erfaren dataskyddssamordnare utses med övergripande ansvar för det operativa dataskyddsarbetet inom stadsdelsförvaltningen. Vidare krävs att ledningsgrupp, ansvariga chefer och utsedda dataskyddsambassadörer får en omfattande dataskyddsutbildning för att kunna ta ansvar för det löpande dataskyddsarbetet som verksamheten kräver. Vidare krävs ett omtag när det gäller styrande dokument och rutiner så att dataskyddsarbetet kan utvecklas av dataskyddssamordnaren i samverkan med övriga nyckelpersoner ISAM och DSO.
Informationsskyldighet		Att lämna tydlig informationen om alla personuppgiftsbehandlingar är en grundläggande förutsättning för all behandling av personuppgifter såväl internt som externt. Det behöver tas fram en extern information som avser de behandlingar som vi inom stadsdelsförvaltningen ansvara för. Den är nödvändig för att vi ska kunna ha egen kontroll över informationen när det sker förändringar i våra behandlingar av personuppgifter. Den kan på samma sätt som information från andra förvaltningar placeras på stadens öppna hemsida. Vidare behöver det tas fram en intern information som rör all personuppgiftsbehandling som sker med personalens personuppgifter och annan intern administration. Denna information ska finnas tillgänglig på stadsdelsförvaltningens interna hemsida.
Behandlingar som sker i stadengemensamma system och tjänster		Stadsdelsförvaltningen bör ges i uppdrag att (i samverkan med övriga stadsdelsförvaltningar) verka för att det sker en tydlig ansvarsuppdelningen inom staden när det gäller personuppgiftsbehandlingar som sker i centrala IT-system och hos andra förvaltningar inom staden. Denna ansvarsuppdelning bör formaliseras genom en tydlig överenskommelse så att alla dataskyddsfrågor kan tas om hand i gemensamma system och i alla utvecklingsprojekt som sker inom staden inte minst vid den pågående digitaliseringen. En sådan ansvarsfördelning måste göras tillgänglig på stadens externa hemsida enligt reglerna i GDPR. Överenskommelsen är viktig för att stadsdelsnämnden ska kunna ta ansvar för ”vår” information även då den

		hanteras av stadens andra förvaltningar och i olika utvecklingsprojekt. Innan en sådan överenskommelse kan komma på plats bör stadsdelsförvaltningen bevaka centrala utvecklingsprojekt som kan komma att, likt projektet kring Miljödata, använda ”vår” information i projekten. Vi måste då kunna klara av att ställa krav på projekten för att skydda ”vår” information och se till att dataskyddsarbetet även i övrigt tas om hand enligt GDPR.

Då Miljödataincidenten ännu inte är färdigutredd kommer den att kommenteras i Bilaga 4 för att lyfta frågor om varför den behöver följas upp. Se även omvärldsbevakningen i Bilaga 2 när det gäller frågor kring Integritetsskyddsmyndighetens (IMYs) inledda tillsyn.

Innehållsförteckning

Inledning

GDPR, eller dataskyddsförordningen, syftar till att skydda individers grundläggande rättigheter och friheter, med särskilt fokus på rätten till skydd av personuppgifter. Dataskyddsreglerna (*kallas GDPR fortsättningsvis*) sätter tydliga ramar för hur personuppgifter får behandlas för att minimera risken för skada och säkerställa att hanteringen sker ansvarsfullt och rättvist. GDPR har sin grund i de mänskliga rättigheterna, där varje individ har rätt till respekt för sitt privat- och familjeliv samt skydd av sina personuppgifter.

Även om Stockholms stad (nedan staden) är en juridisk person har Kommunstyrelsen uttalat att vare nämnd inom Stockholms stad ska anses vara personuppgiftsansvarig för de personuppgifter som hanteras i ”sin verksamhet”. Detta ansvar ska gälla på samma sätt som för personuppgiftsansvarig (alt. biträde) enligt GDPR.

I bilaga 3 ” GDPR:s krav på personuppgiftsansvarig och biträde” anges kortfattat huvuddelen av det ansvar som gäller för personuppgiftsansvariga respektive personuppgiftsbiträde enligt GDPR. Det är detta ansvar som är utgångspunkten vid bedömning av regelefterlevnadsrisker till följd av brister i dataskyddsarbetet i denna rapport.

Dataskyddsombudets uppgift

Varje personuppgiftsansvarig (nämnd eller styrelse) ska utse ett dataskyddsombud. Dataskyddsombudets uppgifter framgår direkt av GDPR och annan lagstiftning. Ombudets roll är att kontrollera att GDPR följs inom organisationen.

Som DSO är den huvudsakliga uppgiften att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad. Det innebär att DSO ska lämna information och råd till verksamheten och de anställda om deras skyldigheter enligt GDPR vid behandling av personuppgifter. Uppdraget ska utföras på ett oberoende sätt. DSO ska vidare rapportera status för dataskyddsarbetet direkt till högsta förvaltningsnivå, vilket görs genom denna årsrapport.

I årsrapporten redogörs för de granskningar och andra observationer som DSO gjort när det gäller verksamhetens status avseende integritet och dataskydd. Årsrapporten är avsedd att ge er som ansvarig för dataskyddsarbetet i verksamheten ett underlag som ni kan använda för uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Tillägg till dataskyddsombudets årsrapport

Hägersten Älvsjö stadsdelsnämnd har valt att ta bort två bilagor från dataskyddsombudets årsrapport. Det rör följande bilagor:

- Bilaga 3: Närmare om GDPR:s krav på ansvarig och biträde
- Bilaga 4: Frågor med anledning av Miljödataincidenten

Båda bilagorna hanterar frågor som ligger utanför nämndens ansvarsområde. Bilaga 3 hanterar Stockholms stads organisation i informationssäkerhetsfrågorna i stort och bilaga 4 hanterar stadens övergripande hantering av Miljödataincidenten. Dessa frågor ligger inom stadsledningskontorets ansvarsområden och nämnden har därför skickat bilagorna till stadsledningskontorets informationssäkerhetsansvariga istället för att bilägga dem nämndens egna årsrapport.

Granskning av dataskyddsarbetet

Kontroll av ”obligatoriska” och andra områden

Dataskyddsombudet har granskat verksamhetens dataskyddsarbete bland annat utifrån sex ”obligatoriska” områden. De sex områdena har identifierats genom en analys av kraven i GDPR om hur verksamheter bör arbeta systematiskt med dataskydd. Varje område innehåller ett antal kontrollfrågor som ger en bild av verksamhetens dataskyddsarbete. Dessa områden överensstämmer med de delar som enligt Integritetsskyddsmyndigheten (IMY) utgör grunden för en verksamhets systematiska och rättssäkra hantering av personuppgifter.

I rapporten används en riskmodell med fyra nivåer av risk. Modellen hjälper dataskyddsombudet att visa vilken bedömning hen gör av verksamhetens dataskyddsrisker utifrån de iakttagelser som gjorts i granskningen.

Risknivå	Beskrivning
Hög risk 	Iakttagelsen avser en brist som kan leda till betydande risker för de registrerades rättigheter och friheter. Bristen kräver omgående åtgärd och korrigering.
Medelhög risk 	Iakttagelsen avser en brist som kan leda till risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas skyndsamt, men kräver inte omedelbar korrigering.
Låg risk 	Iakttagelsen avser en brist som kan leda till mindre risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas, men kräver inte omedelbar korrigering.
Inget att anmärka 	Dataskyddsombudet har inga brister att rapportera avseende denna del.

Notera att risken för att tilldelas en sanktion vid tillsyn är större desto högre risken är.

Resultatsammanställning, iakttagelser inom dataskyddsarbetet

I detta avsnitt presenteras en sammanställning av den bedömda risknivån för verksamhetens dataskyddsarbete, grundat på kontrollfrågorna inom de sex obligatoriska områdena samt ytterligare tre områden. Vidare redovisas dataskyddsombudets centrala iakttagelser, inklusive områden där verksamheten uppvisar goda resultat och bör upprätthålla sitt arbete, samt identifierade brister som kan utgöra dataskyddsrisker. Avsnittet innehåller även dataskyddsombudets rekommenderade åtgärder för att hantera dessa risker och stärka dataskyddsarbetet.

En fullständig redovisning av dataskyddsombudets underlag och resultat från granskningen av de olika områdena finns att läsa i bilaga 1. Bilagan innehåller även en beskrivning av syftet och bakgrunden för varje område.

Register över personuppgiftsbehandlingar

Sammanfattning

Trots att registerförteckningen varit en granskningspunkt sedan GDPR trädde i kraft 2018 så kan det inte sägas vara i nivå med de krav som GDPR ställer upp. Registreringar verkar mest ske av olika typer av handlingar och inte av de mer tydliga personuppgiftsbehandlingarna som sker inom verksamheten. De flesta systemen där behandlingarna sker är inte med i registret och inte heller centrala system där det mesta av den interna verksamheten sker. Det gör det svårt att använda registret för att öka kontrollen över de mer känsliga behandlingarna som sker inom Stadsdelsnämndens verksamhet. Det saknas strategidokument gällande styrning och vägledning när det gäller hur och varför en registrering ska ske. Enligt staden bör registrering av personuppgiftsbehandlingar göras processbaserat och utgå från respektive nämnds hanteringsanvisningar.

Registerförteckningen behöver ses över och bör inriktas emot att göras mer processbaserad än idag för att öka användbarheten och överblicken av de behandlingar som sker inom verksamheten. Det är vidare viktigt att de mest känsliga behandlingarna flaggas upp med riskmarkeringar. Idag saknas ofta uppgift om risknivå i registret.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		Det finns ca 280 registreringar i registret. Omfattningen av registreringarna gör att det är svårt att få en tydlig överblick över verksamhetens behandlingar. Registreringarna har ökat under året vilket kan ses som positivt.
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		I Lokal anvisning för Informationssäkerhet framgår att ISAM har ansvar för registerförteckningen som handhas genom Draftit IT och är ett elektroniskt register Registreringar har genom åren gjorts på olika registerformulär vilket minskar

		överblickbarheten. Det finns en användarmanual för själva registreringen i systemet som är en hjälp för att komma igenom frågorna i registerförteckningen. Det saknas dock ett strategidokument som anger inriktningen när det gäller vad som ska ingå i registerförteckningen. Huvuddelen av posterna är idag olika typer av dokument. Det saknas information om köpta tjänster och de delar av IT-miljön som används för flera behandlingar. Enligt staden bör registrering av personuppgiftsbehandlingar göras processbaserat och utgå från respektive nämnds hanteringsanvisningar
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		Då ansvaret för att se över registerförteckningen är spritt på verksamhetens chefer och då registret inte är processbaserat gör att det är svårt att bedöma om registret verkligen omfattar alla behandlingar som utförs inom verksamheten
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		Det finns vid en ytlig genomgång ett antal uppgifter som kan ifrågasättas eller som inte har angivits.

Säkerhet i samband med behandlingen

Sammanfattning

Informationsklassningar är en verksamhet som har fått förnyad framdrift och sköts på ett bra sätt av informationssäkerhetssamordnaren ISAM. Då det finns en lång lista med system och processer som inte har processats och då arbetet är omfattande kommer informationsklassningen att ta lång tid. Det är bra att ISAM under året har fått en utökad tjänst att ta sig an våra klassningar. I samband med klassningarna sker även en bedömning av om det även är fråga om en personuppgiftsbehandling som kan medföra hög risk för de registrerades friheter och rättigheter. Vid hög risk behöver behandlingen även genomgå en så kallad konsekvensbedömning (se mer nedan)

Informationsklassningen är resurskrävande vilket gör att många system ännu inte är bedömda. En dataskyddssamordnare skulle kunna ta över bedömningen om det behöver genomföras en konsekvensbedömning (vid hög risk) för att öka kontrollen gällande ännu inte informationsklassade processer. Konsekvensbedömningar kan göras åtskilda från informationsklassningen bara det finns någon som kan hålla i genomförandet.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Efter ett antal stickprov på genomförda informations-klassningar, bedömer DSO att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?		Informationsklassningen genomförs på ett bra sätt där ISAM intar en central roll i arbetet. Det finns en god kännedom om olika typer av personuppgifter.
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		Det finns en genomarbetad metodik för klassning i olika situationer som även innefattar en bedömning av om det behöver genomföras en konsekvensbedömning eller inte.
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		Det finns en god kännedom om att informationsklassning ska göras men då det är många datamängder som står på tur att informationsklassas och då det tar tid att genomföra klassningen och uppföljande åtgärder så är det en resursfråga att få klassningarna på plats. Att ISAM övergått till att arbeta med informationssäkerhet på heltid inom Stadsdelsförvaltningen är ett steg i rätt riktning.

Konsekvensbedömning avseende dataskydd

Sammanfattning

Konsekvensbedömningar verkar genomföras endast i samband med de informationsklassningar som ISAM genomför. Vid ett tillfälle har en konsekvensbedömning genomförts vid sidan om den ordningen. Hur många konsekvensbedömningar som genomförts under året är oklart då dessa verkar arkiveras av ansvarig chef på avdelning- eller enhetsnivå efter det att de genomförts. Då konsekvensbedömningar ska omprövas normalt årligen enligt rekommendationer är det oklart hur den uppföljningen ska gå till då det saknas en tydlig förteckning över genomförda bedömningar med anteckning om vem som är ansvarig. Även här borde det finnas en tydlig rutin för hur man ska genomföra och dokumentera de konsekvensbedömningar som är gjorda och när de senast ska revideras. Det förekommer även konsekvensbedömningar som genomförs i sk normerande klassningar av centrala system som är avsedda att användas av flera förvaltningar. Dessa konsekvensbedömningar som sker på central nivå inom staden bör normalt följas upp inom respektive förvaltning för att se till att alla risker inför ett införande i verksamheten har beaktats. Då det förekommer att konsekvensbedömningar inte genomförts i centrala projekt trots att det kan vara fråga om höga risker för den registrerade och att införandeprojekt startar upp utan dessa grundläggande bedömningar är det nödvändigt att följa upp och bevaka att de centrala projekten och annan central utveckling följer GDPR när ”vår” information är avsedd att behandlas i systemen eller tjänsterna.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		Någon särskild rutin finns inte när det gäller när en konsekvensbedömning är aktuell. I klassaverktyget finns det olika klassningar om det gäller en ny behandling. Vid ändring av en behandling görs en annan klassning. En rutin bör övervägas då Lokal anvisning för informationssäkerhet endast berör någon annan situation. Tröskelanalysen borde genomföras för varje behandling.
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		Vid de tröskelanalyser som jag deltagit vid har Integritetsskyddsmyndighetens (IMY) mall för tröskelanalys använts. Den mallen är mindre tydlig än den mall som staden tagit fram varför vi bör överväga att börja använda stadens mall.
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		Det finns mallar framtagna av staden men i de konsekvensbedömningar som jag deltagit i har IMYs mallar använts. Vi bör överväga att pröva stadens mallar för att se vilka som är mest lättillgängliga. IMys risk

		lista är dock en bra utgångspunkt vid riskbedömningen.
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		I och med att konsekvensbedömningar normalt sker samtidigt som det sker en informationsklassning så kommer nödvändiga och klara konsekvensbedömningar att bli liggande i väntan på att informationsklassningen kommer genomföras. Då en övervägande del av processerna och systemen ännu inte har informationsklassats är det en brist som behöver åtgärdas.
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		Det krävs en ändrad organisation av dataskyddsarbetet för att få upp alla behandlingar där det bör göras en konsekvensbedömning. Om det görs en organisationsförändring så att det tillförs en dataskyddssamordnare med ansvar för det operativa dataskyddsarbetet (som föreslås) skulle även behövliga konsekvensbedömningar genomföras på ett strukturerat sätt för att öka kontrollen över de behandlingar som kan medföra hög risk för de registrerades friheter och rättigheter.

Den registrerades rättigheter

Sammanfattning

Enligt Integritetsskyddsmyndigheten IMY är detta område högt prioriterat. Det är viktigt att det finns en tydlig rutin för att fånga upp en begäran från den registrerade. Det är även viktigt att den information som enligt GDPR ska bifogas svaret på en begäran efterlevs. Då denna typ av begäran inte hanteras samlat är det svårt att avgöra omfattningen av dem och om alla begäran hanteras enligt GDPRs krav. Även här saknas en särskild rutin för hur begäran från registrerad ska hanteras och följas upp.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	**Risk**	**Rekommendationer**
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		Såvitt kunnat utredas så verkar det saknas en tydlig rutin för hur en begäran från en registrerad ska hanteras. Ansvaret att hantera dessa ligger på avdelningschefer eller enhetschefer. Det finns dock en rutin för utlämning av allmän handling som nämndkansliet ansvarar för men det gäller olika krav för dessa typer av utlämnande. Det behöver tas fram en tydlig rutin för att hantera en begäran från en registrerad utifrån de krav, inte minst när det gäller information, som framgår av GDPR.
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		Då det saknas en tydlig rutin och då det inte finns några särskilt utsedda handläggare för denna typ av begäran så är det oklart hur många begäran som har inkommit under året.
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		Har inte kontrolleras då det inte sköts sammanhållet.
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		Se ovan. Sannolikt är informationen som ska lämnas i samband med att en begäran besvaras bristfällig.

Personuppgiftsincidenter

Sammanfattning

När det gäller hanteringen av personuppgiftsincidenter i det dagliga arbetet inom förvaltningen så är det händelser som uppmärksammas och hanteras med viss frekvens. Det finns en rutin som anger att DSO ska kontaktas för att den ansvariga chefen ska kunna få en rekommendation om incidenten ska anmälas till IMY. Rutinen anger även att incidentrapportering ska ske i IA-systemet av ansvarig chef. Även här är statistik inte helt lätt att få fram på grund av IA-systemets utformning men det registreras ca en incident i veckan (48 incidenter senaste året). En personuppgiftsincident ska normalt även anmälas in till Integritetsskyddsmyndigheten IMY om vi inte kan visa att det inte har förelegat någon risk för någon fysisk persons friheter och rättigheter. Enligt rutinen ska även nämnden informeras om en incident anmäls till IMY. Om den delen av rutinen är känd inom verksamheten är oklart men ca 80% av incidenterna anmäls även till IMY. Att ha kontroll över de personuppgiftsincidenter som sker inom stadsdelsförvaltningen som helhet är väsentligt för att kunna göra uppföljning och ta lärdom. Även här behövs någon som är ansvarig förslagsvis den föreslagna dataskyddssamordnaren som kan hantera även denna del av det operativa dataskyddsarbetet inom stadsdelsförvaltningen.

Att hantering av personuppgiftsincidenter är tydligt förankrat i verksamheten kan bero på att det är en av de delar av dataskyddsfrågorna som tas upp särskilt i den utbildning kring dataskydd som ska genomföras en gång per år av samtliga anställda inom stadsdelsförvaltningen.

I bedömningen nedan har inte Miljödataincidenten beaktats. Den incidenten ligger på ett annat plan men måste följas upp för att se om vi inom stadsdelsförvaltningen verkligen har gjort allt som vi kunnat för att, om inte förhindrat men väl, begränsa verkningarna av den. Se närmare i Bilaga 4 där ett antal frågor ställs. Det pågår fortfarande olika typer av utredningar kring den varför den bör utredas och bedömas särskilt när dessa är avslutade och då det går att göra en bedömning av hur en liknande incident ska kunna förebyggas eller begränsas särskilt vid den fortsatta digitaliseringen som sker inom stadens centrala verksamhet som alla förvaltningar nyttjar. Även här finns det behov av en förstärkning av det operativa dataskyddsarbetet.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	**Risk**	**Rekommendationer**
Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident?		Det följs upp att personalen genomför sin årliga obligatoriska datasskyddsutbildning där personuppgiftsincidenter tas upp särskilt. Det rör frågor som är enkla att ta till sig då vi hanterar mycket känsliga data inom verksamheten.
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella		I den dagliga verksamheten fungerar det bra. Det finns en rutin men om det rapporteras

personuppgiftsincidenter? Följs dessa?		till nämnden vid anmälan till IMY är oklart och har inte följts upp.
Hur många personuppgiftsincidenter har dokumenterats under året?		Enligt en rapport som tagits fram i IA-systemet så finns det 48 registrerade incidenter. Sannolikt kan det röra sig om fler incidenter men som registrerats under annan rubrik.
Hur många personuppgiftsincidenter har anmälts till IMY under året?		Här finns det en osäkerhet då incidenter hanteras av avdelningscheferna och det inte finns någon ansvarig för att följa upp vilka som anmäls till IMY. Uppskattningsvis bör minst fyra av fem ha anmälts till IMY och därmed även till nämnden. Det borde under året röra sig om ett fyrtiotal.

Överföring till tredje land

Sammanfattning

I takt med att digitaliseringen ökar inom staden och då fler tjänster flyttas från att hanteras lokalt av centrala IT inom staden till olika typer av molnbaserade tjänster kommer tredjelandsöverföringar (dvs överföringar av personuppgifter till länder utanför EU/EES) att öka och bli vanligare. Vid en sådan överföring krävs det en särskild utredning om vilka skyddsåtgärder som kan vidtas beroende av vilka länder som är aktuella. Det man kommer överens om vid överföringen regleras normalt i personuppgiftsbiträdesavtal i samband med det tjänsteavtal som träffas angående tjänsterna. Det finns ingen rutin för hur sådana tredjelandsöverföringar ska hanteras inom stadsdelsförvaltningen. I dagsläget verkar personuppgiftsbiträdesavtalen hanteras av avdelnings- eller enhetschefer. När det gäller centrala tjänster som rör flera förvaltningar borde det finnas avtal som stadsdelsförvaltningen bör kunna få del av och följa upp innan vi använder tjänsterna för ”vår” information. Inte heller här finns det någon rutin om hur det ska hanteras. Behovet av en dataskyddssamordnare är tydligt även här.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		Det finns några anteckningar i registerförteckningen med någon närmare uppföljning har inte genomförts. Då det saknas en stor del av oklassade system i registerförteckningen är det sannolikt att

		det då finns olika tredjelandsöverföringar som vi inte har kontroll över.
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		Det saknas rutiner för hantering av personuppgiftsbiträdesavtal varför det är sannolikt att dessa frågor ej har hanterats.
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		Har inte träffat på någon ”TIA” under min tid inom stadsdelsförvaltningen.

Ansvarsskyldigheten

Sammanfattning

Vid genomgång av olika granskningsområden blir det tydligt att det saknas ett organiserat operativt dataskyddsarbete inom stadsdelsförvaltningen som kan hålla ihop alla dataskyddsfrågor som måste hanteras inom en verksamhet för att kunna leva upp till alla de krav som dataskyddsförordningen GDPR kräver. Som personuppgiftsansvarig måste man även kunna visa att man efterlever GDPR regelverk. Även Miljödataincidenten indikerar att vi sannolikt inte har den kontroll som vi borde ha haft när det gäller alla de personuppgifter som rör våra anställda och tidigare anställda.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig kontroll över de personuppgiftsbehandlingar som sker i verksamheten och kan visa att man lever upp till de krav som GDPR ställer upp?		Det finns inte något organiserat operativt dataskyddsarbete men en utpekad ansvarig vilket gör att dataskyddsarbetet sker vid behov och dokumenteras inte på ett samlat sätt som visar hur vi har tagit oss an dataskyddsfrågorna över tid.
Är den organisation av dataskyddsarbetet som finns tillräcklig för att hantera alla krav som ställs av GDPR i verksamheten inom stadsdelsförvaltningen?		Nej är det korta svaret. Det behöver utses en erfaren dataskyddssamordnare med ett övergripande ansvar för det operativa arbetet med dataskyddsfrågor och som kan införa rutiner och strategidokument samt stödja verksamheten med alla praktiska frågor. Dataskyddssamordnaren ska även ansvara för att det sker en samordning inom staden när det gäller system och

		tjänster som rör flera förvaltningar samt vid utvecklingsprojekt.

Informationsskyldigheten

Sammanfattning

Det finns omfattande brister när det gäller dels tillgängligheten på information om de behandlingar av personuppgifter som sker inom verksamheten och i den interna administrationen dels innehållet och möjligheten att ändra innehållet efter de förutsättningar som vid var tid gäller för de behandlingar som sker. Tydlig samlad information om alla våra behandlingar som sker i verksamheten bör tas fram och publiceras på stadens publika hemsida och motsvarande information om de interna personuppgiftsbehandlingarna ska tas fram och göras tillgänglig på våra interna sidor så att den är lättillgänglig för all personal som berörs av den. Det ska finnas någon som är ansvarig för att hålla informationen uppdaterad och innehålla de delar som framgår av GDPR.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Hanterar vi informationskraven enligt GDPR?		Den information som finns på stadens sidor är inte fullständig och inte anpassad till vår stadsdelsförvaltnings verksamhet. Vi kan inte heller förändra innehållet i den informationen för att leva upp till de krav som finns i GDPR. När det gäller den interna informationen så saknas det en samlad information om alla behandlingar som sker i verksamheten och som ska vara lättillgänglig för all personal. Även här är behovet av en ansvarig dataskyddssamordnare tydligt.

Ansvar för behandlingar i stadens och andra förvaltningars tjänster

Sammanfattning

Det saknas någon ansvarig som kan bevaka och följa upp att dataskyddsarbetet genomförs enligt GDPR gällande de system och tjänster som förvaltas centralt inom staden eller på annan förvaltning men där ”våra” uppgifter behandlas för vår räkning. Vi måste försäkra oss om att den verksamheten sker enligt gällande regler enligt GDPR och kunna ställa krav på lämpliga skyddsåtgärder. Motsvarande gäller även för de utvecklingsprojekt som sker utanför

vår stadsdelsnämnd men där ”vår” information kommer att hanteras (jämför med Miljödata). Även här är det tydligt att det krävs att det finns en ansvarig dataskyddsamordnare som kan hantera dessa frågor åt stadsdelsförvaltningen. Innan en sådan person är på plats är det ledningen som bör hantera dessa frågor så att skyddet av ”våra” personuppgifter kan upprätthållas.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig kontroll över sin information som hanteras i centrala system eller i utveckling inom staden utanför stadsdelsnämnden?		Som personuppgiftsansvarig har stadsdelsnämnden ansvaret att se till att ”våra” personuppgifter är tillräckligt skyddade och att vi kan ge de instruktioner som är nödvändiga för att ha kontrollen över vår information även om den hanteras i centrala system och utvecklingsprojekt. Även här bör en ansvarig dataskyddssamordnare fylla en viktig funktion i det operativa dataskyddsarbetet som är nödvändigt mot bakgrund av reglerna i GDPR.

Bilagor

Bilaga 1: Detaljerad redovisning av dataskyddsombudets granskning

Bilaga 2: Omvärldsbevakning i korthet

Bilaga 1 - Detaljerad redovisning av dataskyddsombudets granskning

Denna bilaga innehåller en beskrivning av syftet med respektive obligatoriskt område samt en mer detaljerad redovisning av granskning och slutsatser. Här framgår vilka iakttagelser som gjorts och vilken information som samlats in under granskningsarbetet dels av de sex obligatoriska rapporteringsområdena samt av de tre särskilda granskningsområden som lagts till då de har stor betydelse för ett strukturerat löpande dataskyddsarbete. För varje område redovisas de underlag som har använts, de iakttagelser som har gjorts samt hur dessa har utgjort grunden för dataskyddsombudets riskbedömning och rekommenderade åtgärder. När det gäller flera områden har granskningen skett genom deltagande i verksamhetens dataskyddsarbete varför inte varje område är dokumenterat till fullo.

Presentation av DSO och arbetssätt

Mitt namn är Christian Sandell och jag är dataskyddsombud (DSO) sedan mitten av augusti i år på 20 % av en heltid enligt ett ramavtal som gällt i många år. I praktiken har jag till följd av incidenter och många möten kring informationsklassningar och konsekvensbedömningar mm kommit att arbeta ca 30 % av heltid. Då merparten av arbetet legat på möten och hantering av incidenter har medfört att jag haft begränsad tid för att på djupet lära känna alla delar av dataskyddsarbetet som sker inom stadsdelsförvaltningen. Jag har tidigare arbetat som dataskyddsombud i olika fackförvaltningar inom staden under ett drygt halvår vilket medfört att jag är bekant med hur dataskyddsarbete bedrivs inom staden. Jag har djupa kunskaper inom GDPR med följdlagstiftning och praxis och har sedan ikraftträdandet i maj 2018 arbetat med dataskyddsfrågor på heltid som dataskyddsombud och som dataskyddsansvarig främst inom privat sektor men även inom offentlig sektor. Mitt uppdrag kommer upphöra vid årsskiftet.

För mig handlar dataskyddsarbete om att visa respekt för de mänskor vars personuppgifter vi samlar in och hanterar för olika syften.

När vi använder besökandes, brukares och anställdas personuppgifter måste vi ha kunskap om och kontroll över personuppgifterna. Vi ska kunna skydda dem genom ett organiserat arbetssätt, säkra systemlösningar och ansvarstagande samarbetspartners. Dataskyddsarbetet är en kontinuerlig process där vi regelbundet ska ompröva all användning av personuppgifter så att vi inte behandlar mer uppgifter än som är nödvändigt för att nå de ändamål som vi samlade in uppgifterna för. Vi ska även löpande bedöma riskerna för de registrerades friheter och rättigheter inklusive skyddet av personuppgifter. Vi ska informera brukare och anställda om alla våra behandlingar på ett öppet och tydligt sätt. Utgångspunkten för dataskyddsarbetet är en uppdaterad registerförteckning som ger överblick och kontroll och där det framgår vem som är ansvarig för respektive behandling.

Som DSO har jag samlat information om hur vi behandlar personuppgifter inom stadsdelsförvaltningen genom att delta i det dataskyddsarbete som förekommer. Detta är ett viktigt led i arbete för att jag ska kunna ge råd och stöd om skyldigheterna enligt GDPR till verksamheten.

En av de främsta uppgifterna som DSO har är att övervaka efterlevnaden av GDPR inom verksamheten och hur vi följer våra interna strategidokument. Jag har utgått från stadens styrande dokument för att förstå hur ansvaret har fördelats och även tagit del av Lokal anvisning för informationssäkerhet och delegationsordningen för att veta hur vi organiserat dataskyddsarbetet. Slutsatsen blir att huvudansvaret för det operativa dataskyddsarbetet har

formellt lagts på förvaltningsdirektören men det huvudsakliga faktiska dataskyddsarbetet utförs av alla avdelnings- och enhetschefer. Även informationssäkerhetssamordnaren ISAM har ett ansvar för delar av dataskyddsarbetet men har inte ansvar för alla delar.

En viktig observation som gjorts är att dataskyddsarbetet fortfarande huvudsakligen är inriktat på att hantera behandlingar som varit igång sedan GDPR infördes. Det är först när nya behandlingar ska in i dataskyddsarbetet som bristerna i det operativa arbetet blir tydliga.

1. Register över personuppgiftsbehandlingar

Syftet med området

I GDPR framkommer det att personuppgiftsansvariga (och personuppgiftsbiträden) ska föra ett register över sina personuppgiftsbehandlingar. Registret brukar benämnas ”behandlingsregister” eller ”registerförteckning”. Registret ska finnas tillgängligt i elektronisk form och ska omfatta samtliga personuppgiftsbehandlingar som personuppgiftsansvarig utför. Det ska hållas uppdaterat vilket innebär att det ska uppdateras vid nya eller förändrade personuppgiftsbehandlingar.

Syftet med detta rapporteringsområde är att rapportera om verksamheten har ändamålsenliga rutiner som möjliggör att nya/förändrade personuppgiftsbehandlingar registreras, huruvida personuppgiftsbehandlingar registreras/uppdateras såsom det krävs samt huruvida de uppgifter som är obligatoriska har besvarats kopplat till de registrerade personuppgiftsbehandlingarna.

Kontroller och iakttagelser gjord av dataskyddsombudet

Antal behandlingar som är registrerade?

Det finns ca 280 registreringar i registret.

Omfattningen av registreringarna gör att det är svårt att få en tydlig överblick över verksamhetens behandlingar. Registreringarna har ökat under året vilket kan ses som positivt.

Vid en ytlig granskning av registret framkommer att det huvudsakligen olika typer av listor som registrerats i registret och att de flesta centrala behandlingsystem inte finns med i registret. Det finns till exempel 19 registerposter som avser semesterlistor 4 personallista, 7 telefonlista etc.

Har verksamheten ändamålsenliga rutiner som möjliggör att nya/förändrade behandlingar registreras?

I Lokal anvisning för Informationssäkerhet framgår att ISAM har ansvar för registerförteckningen som handhas genom Draftit IT och är ett elektroniskt register

Registreringar har genom åren gjorts på olika registerformulär vilket minskar överblickbarheten. Det finns en användarmanual för själva registreringen i systemet som är en hjälp för att komma igenom frågorna i registerförteckningen.

Det saknas dock ett strategidokument som anger inriktningen när det gäller vad som ska ingå i registerförteckningen. Huvuddelen av posterna är idag olika typer av dokument. Det saknas information om köpta tjänster och de delar av IT-miljön som används för flera behandlingar.

Enligt staden bör registrering av personuppgiftsbehandlingar göras processbaserat och utgå från respektive nämnds hanteringsanvisningar.

Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?

Då ansvaret för att se över registerförteckningen är spritt på verksamhetens chefer och då registret inte är processbaserat gör att det är svårt att bedöma om registret verkligen omfattar alla behandlingar som utförs inom verksamheten. Det är snarare så att det ganska klart framgår att det saknas stora delar av behandlingarna på ett strukturerat sätt i registret.

Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?

Det finns vid en ytlig genomgång ett antal uppgifter som kan ifrågasättas eller som inte har angivits. Det finns bland angivet som en rättslig grund på ett antal behandlingar berättigat intresse det vill säga den rättsliga grunden ”intresseavvägning” trots att det i princip inte finns utrymme att använda den grunden inom offentlig sektor för behandlingar som utförs för att fullgöra sina uppgifter.

Dataskyddsombudets bedömning samt rekommendationer

Registerförteckningen behöver ses över och bör inriktas emot att göras mer processbaserad än idag för att öka användbarheten och överblicken av de behandlingar som sker inom verksamheten. Det är vidare viktigt att de mest känsliga behandlingarna flaggas upp med riskmarkeringar. Idag saknas ofta uppgift om risknivå i registret.

2. Säkerhet i samband med behandlingen

Bakgrund och syfte

Personuppgiftsansvarig ska tillse att personuppgifter skyddas med lämpliga säkerhetsåtgärder, detta för att till exempel undvika att obehöriga får tillgång till uppgifterna eller att uppgifterna förloras.

Personuppgiftsansvarig behöver bedöma vilka tekniska- och organisatoriska säkerhetsåtgärder som ska vidtas för de behandlingar som utförs. Till tekniska säkerhetsåtgärder räknas till exempel kryptering, pseudonymisering och säkerhetskopiering. Organisatoriska säkerhetsåtgärder avser till exempel interna riktlinjer och rutiner.

För att skapa förutsättningar för att skydda information (inklusive personuppgifter) med rätt slags skydd ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare. Genom riskanalyser identifierar informationsägaren risker och väljer åtgärder för att minska riskerna. Risker i samband med personuppgiftsbehandling är en typ av risk som informationsägaren behöver omhänderta i riskanalyser.

Att det finns skriftliga, beslutade och kommunicerade styrdokument samt kända rutiner medför att medarbetarna vet hur de ska agera avseende frågor som rör dataskydd. Den personuppgiftsansvariga måste kunna *visa* hur GDPR efterlevs och att det finns styrdokument och rutiner är en viktig del i detta (en del av ansvarsskyldigheten).

Syftet med detta rapporteringsområde är därmed att rapportera huruvida DSO bedömer att det tas hänsyn till risker för den registrerade och om dessa beaktas i tillräcklig mån i genomförda informationsklassningar och riskanalyser. Vidare bedömer DSO huruvida det finns tillräckligt

mycket reglerat om dataskydd i styrdokument och rutiner samt om dessa är tillräckligt implementerade och kända.

Kontroller och iakttagelser gjord av dataskyddsombudet

Efter ett antal stickprov på genomförda informationsklassningar, bedömer DSO att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?

Informationsklassningen genomförs på ett bra sätt där ISAM intar en central roll i arbetet.

Det finns en god kännedom om olika typer av personuppgifter

Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?

Det finns en genomarbetad metodik för klassning i olika situationer som även innefattar en bedömning av om det behöver genomföras en konsekvensbedömning eller inte.

Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?

Det finns en god kännedom om att informationsklassning ska göras men då det är många datamängder som står på tur att informationsklassas och då det tar tid att genomföra klassningen och uppföljande åtgärder så är det en resursfråga att få klassningarna på plats. Att ISAM övergått till att arbeta med informationssäkerhet på heltid inom stadsdelsförvaltningen är ett steg i rätt riktning.

Dataskyddsombudets bedömning samt rekommendationer

Informationsklassningen är resurskrävande vilket gör att många system ännu inte är bedömda. En dataskyddssamordnare skulle kunna ta över bedömningen om det behöver genomföras en konsekvensbedömning (vid hög risk) för att öka kontrollen gällande ännu inte informationsklassade processer. Konsekvensbedömningar kan göras åtskilda från informationsklassningen bara det finns någon som kan hålla i genomförandet.

3. Konsekvensbedömning avseende dataskydd

Bakgrund och syfte

En konsekvensbedömning avseende dataskydd krävs när personuppgiftsansvarig planerar att inleda en personuppgiftsbehandling som innebär hög risk för de registrerade. Huruvida en behandling innebär hög risk eller inte behöver personuppgiftsansvarig avgöra genom att genomföra en s.k. tröskelanalys.

En konsekvensbedömning ska vara genomförd för samtliga behandlingar som innebär hög risk, vilket innebär att personuppgiftsansvarig även behöver kontrollera huruvida denne utför befintliga behandlingar som innebär hög risk. Om högriskbehandlingar utfös för vilka en konsekvensbedömning inte har gjorts, behöver personuppgiftsansvarig genomföra en sådan.

Genom att genomföra en konsekvensbedömning kan personuppgiftsansvarig identifiera risker med en personuppgiftsbehandling, hantera riskerna genom åtgärder och rutiner samt påvisa ansvarsskyldighet. Genom konsekvensbedömningar kan risker identifieras och förebyggas.

Syftet med detta rapporteringsområde är att rapportera huruvida verksamheten har ändamålsenliga rutiner som möjliggör att tröskelanalyser och konsekvensbedömningar

genomförs, huruvida sådana genomförs när det krävs samt huruvida personuppgiftsansvarig har genomfört konsekvensbedömningar för de behandlingar som kräver det.

Kontroller och iakttagelser gjord av dataskyddsombudet

Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?

Enligt Lokal anvisning för Informationssäkerhet ligger ansvaret för att genomföra konsekvensbedömningar på Avdelningschefsnivå.

Någon särskild rutin finns inte när det gäller när en konsekvensbedömning är aktuell. I klassaverktyget finns det olika klassningar om det gäller en ny behandling. Vid ändring av en behandling görs en annan klassning.

En rutin bör övervägas då Lokal anvisning för informationssäkerhet endast berör någon annan situation. Tröskelanalysen borde genomföras för varje behandling.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

Vi de tröskelanalyser som jag deltagit vid har Integritetsskyddsmyndigheten (IMY) mall för tröskelanalys använts. Den mallen är mindre tydlig än den mall som staden tagit fram varför vi bör överväga att börja använda stadens mall.

Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?

Det finns mallar framtagna av staden men i de konsekvensbedömningar som jag deltagit i har IMYs mallar använts.

Vi bör överväga att pröva stadens mallar för att se vilka som är mest lättillgängliga. IMys risk lista är dock en bra utgångspunkt vid riskbedömningen.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

I och med att konsekvensbedömningar normalt sker samtidigt som det sker en informationsklassning så kommer nödvändiga och klara konsekvensbedömningar att bli liggande i väntan på att informationsklassningen kommer genomföras.

Då en övervägande del av processerna och systemen ännu inte har informationsklassats är det en brist som behöver åtgärdas.

Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?

Det krävs en ändrad organisation av dataskyddsarbetet för att få upp alla behandlingar där det bör göras en konsekvensbedömning. Om det göras en organisationsförändring så att det tillförs en dataskyddssamordnare med ansvar för det operativa dataskyddsarbetet (som föreslås) skulle även behövliga konsekvensbedömningar genomföras på ett strukturerat sätt för att öka kontrollen över de behandlingar som kan medföra hög risk för de registrerades friheter och rättigheter.

Dataskyddsombudets bedömning samt rekommendationer

Då konsekvensbedömningar ska omprövas normalt årligen enligt rekommendationer är det oklart hur den uppföljningen ska gå till då det saknas en tydlig förteckning över genomförda bedömningar med anteckning om vem som är ansvarig. Även här borde det finnas en tydlig rutin för hur man ska genomföra och dokumentera de konsekvensbedömningar som är gjorda och när de senast ska revideras. Det förekommer även konsekvensbedömningar som genomförs i sk normerande klassningar av centrala system som är avsedda att användas av flera förvaltningar. Dessa konsekvensbedömningar som sker på central nivå inom staden bör normalt följas upp inom respektive förvaltning för att se till att alla risker inför ett införande i verksamheten har beaktats. Då det förekommer att konsekvensbedömningar inte genomförts i centrala projekt trots att det kan vara fråga om höga risker för den registrerade och att införandeprojekt startar upp utan dessa grundläggande bedömningar är det nödvändigt att följa upp och bevaka att de centrala projekten och annan central utveckling följer GDPR när ”vår” information är avsedd att behandlas i systemen eller tjänsterna.

4. Den registrerades rättigheter

Bakgrund och syfte

Den registrerade har ett antal rättigheter enligt GDPR. Den registrerade kan bland annat begära tillgång (registerutdrag), rättelse eller radering. Den som är personuppgiftsansvarig har att tillmötesgå en begäran enligt de krav som finns.

Syftet med detta rapporteringsområde är att kontrollera huruvida det finns ändamålsenliga mallar samt rutiner för besvarande av rättighetsbegäran, huruvida inkomna begäranden har hanterats inom den tidsram som finns att förhålla sig till samt huruvida svaren till de registrerade, baserat på ett antal stickprov, uppfyller lagkraven.

Kontroller och iakttagelser gjord av dataskyddsombudet

Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?

Såvitt kunnat utredas så verkar det saknas en tydlig rutin för hur en begäran från en registrerad ska hanteras. Ansvaret att hantera dessa ligger på avdelningschefer eller enhetschefer. Det finns dock en rutin för utlämning av allmän handling som nämndkansliet ansvarar för men det gäller olika krav för dessa typer av utlämnande.

Det behöver tas fram en tydlig rutin för att hantera en begäran från en registrerad utifrån de krav, inte minst när det gäller information, som framgår av GDPR.

Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?

Då det saknas en tydlig rutin och då det inte finns några särskilt utsedda handläggare för denna typ av begäran så är det oklart hur många begäran som har inkommit under året.

Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?

Har inte kunnat kontrolleras då det inte sköts sammanhållet.

Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?

Se ovan. Sannolikt är informationen som ska lämnas i samband med att en begäran besvaras bristfällig.

Dataskyddsombudets bedömning samt rekommendationer

Enligt Integritetsskyddsmyndigheten IMY är detta område högt prioriterat. Det är viktigt att det finns en tydlig rutin för att fånga upp en begäran från den registrerade. Det är även viktigt att den information som enligt GDPR ska bifogas svaret på en begäran efterlevs. Då denna typ av begäran inte hanteras samlat är det svårt att avgöra omfattningen av dem och om alla begäran hanteras enligt GDPRs krav. Även här saknas en särskild rutin för hur begäran från registrerad ska hanteras och följas upp.

5. Personuppgiftsincidenter

Bakgrund och syfte

Med begreppet personuppgiftsincident avses en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Om en inträffad personuppgiftsincident medför en risk för fysiska personers rättigheter och friheter ska den anmälas till Integritetsskyddsmyndigheten (IMY) inom 72 timmar från upptäckt. Om personuppgiftsincidenten sannolikt leder till hög risk för de registrerade måste de informeras utan onödigt dröjsmål.

Om en personuppgiftsincident inte bedöms vara anmälningspliktig ska den dokumenteras.

Syftet med detta rapporteringsområde är att kontrollera huruvida det säkerställs att samtliga medarbetare har den kunskap som krävs om personuppgiftsincidenter, huruvida det finns ändamålsenliga rutiner för att hantera händelser som kan utgöra personuppgiftsincidenter och huruvida dessa rutiner följs.

Kontroller och iakttagelser gjord av dataskyddsombudet

Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident?

Det följs upp att personalen genomför sin årliga obligatoriska datasskyddsutbildning där personuppgiftsincidenter tas upp särskilt.

Det rör frågor som är enkla att ta till sig då vi hanterar mycket känsliga data inom verksamheten.

Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?

I den dagliga verksamheten fungerar det bra. Det finns en rutin men om det rapporteras till nämnden vid anmälan till IMY är oklart och har inte följts upp.

Hur många personuppgiftsincidenter har dokumenterats under året?

Enligt en rapport som tagits fram i IA-systemet så finns det 48 registrerade incidenter.

Sannolikt kan det röra sig om fler incidenter men som registrerats under annan rubrik.

Hur många personuppgiftsincidenter har anmälts till IMY under året?

Här finns det en osäkerhet då incidenter hanteras av avdelningscheferna och det inte finns någon ansvarig för att följa upp vilka som anmäls till IMY. Uppskattningsvis bör minst fyra av fem ha anmälts till IMY och därmed även till nämnden. Det borde under året röra sig om ett fyrtiotal.

Dataskyddsombudets bedömning samt rekommendationer

Detta område är det område förutom informationsklassning där det sker ett dataskyddsarbete inom verksamheten som är värd att nämna. Att fortsätta på den inslagna vägen är viktigt och att området är ett av några som ingår i den obligatorisk utbildningen visar att repetition och utbildning är viktiga inslag i denna typ av arbete.

6. Överföring till tredje land

Bakgrund och syfte

För att säkerställa att den nivå av skydd för personuppgifter som ställs i GDPR inte undergrävs får överföringar av personuppgifter till länder utanför EU/EES (tredje land) endast ske under särskilda förutsättningar. Det innebär att sådan överföring måste stödjas på antingen ett beslut från EU-kommissionen om att landet ifråga upprätthåller en adekvat skyddsnivå, att överföringen omfattas av en lämplig skyddsåtgärd eller i särskilda undantagsfall. Vidare behöver även kompletterade skyddsåtgärder, utöver de lämpliga skyddsåtgärderna, vidtas i vissa fall.[1]

Syftet med detta rapporteringsområde är att rapportera huruvida personuppgiftsansvarig har identifierat de tredjelandsöverföringar som utförs, huruvida personuppgiftsansvarig tillämpar överföringsverktyg på de tredjelandsöverföringar som utförs och om nödvändiga bedömningar har gjorts avseende tredjelandsöverföringarna.

Kontroller och iakttagelser gjord av dataskyddsombudet

Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?

Det finns några anteckningar i registerförteckningen med någon närmare uppföljning har inte genomförts. Då det saknas en stor del av oklassade system i registerförteckningen är det sannolikt att det då finns olika tredjelandsöverföringar som vi inte har kontroll över.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

Det saknas rutiner för hantering av personuppgiftsbiträdesavtal varför det är sannolikt att dessa frågor ej har hanterats.

Har nödvändig bedömning, ”Transfer Impact Assessment” (TIA), gjorts avseende tredjelandsöverföringarna?

Har inte träffat på någon TIA under min tid inom stadsdelsförvaltningen.

Dataskyddsombudets bedömning samt rekommendationer

I takt med att digitaliseringen ökar inom staden och då fler tjänster flyttas från att hanteras lokalt av centrala IT inom staden till olika typer av molnbaserade tjänster kommer

[1] Europeiska dataskyddsstyrelsens (EDPB) Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överenstämmelsen med EU-nivån för skydd av personuppgifter, Version 2.0, Antagna den 18 juni 2021.

tredjelandsöverföringar att öka och bli vanligare. Vid en sådan överföring krävs det en särskild utredning om vilka skyddsåtgärder som kan vidtas beroende av vilka länder som är aktuella. Det finns ingen rutin för hur tredjelandsöverföringar ska hanteras inom stadsdelsförvaltningen. I dagsläget verkar personuppgiftsbiträdesavtalen hanteras av avdelnings- eller enhetschefer. När det gäller centrala tjänster som rör flera förvaltningar borde det finnas avtal som stadsdelsförvaltningen bör kunna få del av och följa upp innan vi använder tjänsterna för ”vår” information. Inte heller här finns det någon rutin om hur det ska hanteras. Behovet av en dataskyddssamordnare är tydligt även här.

7. Personuppgiftsansvarigs ansvarsskyldighet

Bakgrund och syfte

Enligt GDPR (art 5:2) har den personuppgiftsansvarige ett ansvar för att alla grundläggande dataskyddsprinciper efterlevs gällande all personuppgiftsbehandling i en verksamhet. Den personuppgiftsansvarige ska vidare (se art 24:1) med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa att behandlingen utförs i enlighet med GDPR. Dessa åtgärder ska ses över och uppdateras vid behov. Den personuppgiftsansvarige ska vidare kunna visa att all behandlingen utförs i enlighet med GDPR. Det innebär att alla frågor och andra överväganden som rör arbetet med dataskydd behöver dokumenteras för framtiden.

Syftet med detta rapporteringsområde är att rapportera huruvida personuppgiftsansvarig har vidtagit de åtgärder som är nödvändiga för att det löpande operativa dataskyddsarbetet är organiserat på ett ändamålsenligt sätt så att skyddet av personuppgifter kan upprätthållas på en lämplig nivå med hänsyn till de risker som finns i verksamheten. Det ska vidare finnas en centralt tillgänglig lagringsyta där bland annat alla beslut, rutiner, sammanställningar, konsekvensbedömningar, ställningstaganden etc finns samlat. Så att uppföljning av arbetet kan göras och så att vi vet vilka ställningstaganden som fattats och vilka mallar, rutiner, anvisningar etc som finns som man inom verksamheten har behov av att veta och följa upp när det gäller dataskyddsarbetet.

Kontroller och iakttagelser gjord av dataskyddsombudet

Som personuppgiftsansvarig har varje nämnd det operativa ansvaret för att verksamheten är organiserad och har tillräckliga resurser för att kunna leva upp till GDPR:s krav vid all hantering av personuppgifter inom sin verksamhet.

Staden har valt att lägga in dataskyddarbetet som en del inom arbetet med informationssäkerhet. Även om det finns tydliga beröringspunkter mellan dessa regelverk så finns det delar av dataskyddsarbetet som ställer andra krav och som i vissa delar (såsom reglerna i GDPR är utformade) kan komma att hamna i strid med vad som anses som bra informationssäkerhet. Dataskyddsarbete avser förenklat uttryckt att skydda de registrerades friheter och rättigheter till skillnad mot informationssäkerhet som avser att skydda verksamhetens informationstillgångar.

Dataskyddsarbetet inom staden har, efter det att införandeprojektet avslutades 2019, formats lokalt inom respektive förvaltning vilket har medfört att delar av dataskyddsarbetet enligt GDPR fungerar men att andra delar har försummats eller inte har beaktats. Det delegerade ansvaret för det operativa dataskyddsarbetet har inte ökat skyddet av personuppgifter då kunskapsnivån om det omfattande regelverket är generellt för låg.

När det gäller stadsdelsförvaltningen är detta förhållande tydligt då det fortfarande inte finns en organisation för att kunna hantera alla de krav som GDPR ställer upp för en verksamhet när det gäller det operativa dataskyddsarbetet.

Inte ens de delar som har omfattats av de obligatoriska rapporteringsområdena har efter flera års påpekande kommit i ordning. Det finns fortfarande inte en registerförteckning som uppfyller kraven. Registerförteckningen är omfattande men innehåller främst olika typer av handlingar och inte de beståndsdelar som är viktiga för att förstå var olika processer sker och i vilka system och med hjälp av olika typer av köpta eller inom staden utvecklade tjänster och system. Registret är inte komplett och det saknas en tydlig struktur över hur olika behandlingar bör föras in i registret. Förteckningen ska kunna lämnas ut till IMY vid en granskning.

Stadsdelsförvaltningens organiserade dataskyddsarbete är uppbyggt kring några få nyckelpersoner vilket har gjort och gör det sårbart. Enligt Lokal anvisning för informationssäkerhet är ansvaret för informationen som hanteras inom verksamheten fördelad mellan förvaltningsdirektören ner till avdelning/enhetschefnivånivå beroende av om informationen behandlas inom hela förvaltningen eller endast inom en viss avdelning eller enhet. Det är informationsägare ofta avdelningschefer eller enhetschefer som har ett särskilt ansvar för att informationen hanteras enligt gällande lagstiftning och riktlinjer.

Det finns någon enstaka rutin som är beslutad i nämnden. Det förekommer att man använder andra stadsdelsnämnders rutiner i brist på egna vilket visar på att det saknas ett organiserat operativt dataskyddsarbete. Arbetet är ofta reaktivt och inte framåtsyftande.

Enligt staden har Informationssäkerhetssamordnaren (ISAM) och DSO ansetts vara de personer/funktioner som haft ansvaret att driva dataskyddsarbetet framåt från start. Denna uppfattning har hämmat utvecklingen då DSO inte kan ha det operativa ansvaret och samtidigt agera på oberoende basis och granska samma dataskyddsarbete. Trots att Stadsrevision i sin granskning redan 2019 (av implementeringen av dataskyddsarbetet) poängterade att ”dataskyddsombudet ska ha en reviderande och rådgivande roll och inte delta i det operativa arbetet med behandling av personuppgifter som till exempel inventering och upprättande av registerförteckning.” (se sid 5 i Stadsrevisions rapport nr 5, 2019) så gick utvecklingen åt ett annat håll.

Det är först i år som synen på dataskyddsombudets roll inom staden på allvar har definierats till att vara den dataskyddsrevisor som på ett oberoende, granskande och uppföljande sätt tar tillvara de registrerades fri- och rättigheter i granskningen av stadsdelsnämndens dataskyddsarbete.

Att nämnden ska utgå ifrån DSO:s årsrapport för att besluta om det framtida dataskyddsarbetet skapar en passiv inställning till ansvarsfrågan. Operativt dataskyddsarbete ska inte vara reaktivt utan proaktivt då dataskyddsfrågorna måste beaktas innan exempelvis en tjänst köps in eller utvecklas. Att vi bara har arbetat med befintliga system och personuppgiftsbehandlingar under alla år är ett stort svaghetstecken i dataskyddsarbetet och när vi börjar ta oss an nya behandlingar och tjänster blir bristerna uppenbara.

Dataskyddsarbete är komplext då det spänner över många områden och då det kräver samverkan från olika funktioner inom en verksamhet som juridik, IT, Informationssäkerhet, DSO, kommunikation, inköp och upphandling, projekt och administration. Även kontakten med alla objektägare som finns såväl i den egna verksamheten som inom staden är väsentlig i ett löpande operativt dataskyddsarbete.

Det finns idag betydande brister i organisationen av stadsdelsförvaltningens dataskyddsarbete vilket framgår vid närmare genomgång av de olika granskningsområdena. Det är viktigt att påpeka att de personer som jag haft kontakt med och samverkat med har alla visat på god vilja att förstå och arbeta för att förbättra dataskyddsarbetet inom förvaltningen.

I min bedömning utgår jag från de krav som GDPR ställer upp på en personuppgiftsansvarig (se Bilaga 3) varför jag drar slutsatsen att det operativa dataskyddsarbetet inom stadsdelsförvaltningen inte är organiserat så att det kan klara av att leva upp till alla krav som ställs. Ansvarsskyldigheten är omfattande och det är nödvändigt att dataskyddsarbetet är organiserat och bemannat så att dataskyddsfrågorna kan hanteras löpande i en verksamhet och även hållbart över tid.

Dataskyddsombudets bedömning samt rekommendationer

För stadsdelsförvaltningens del är situationen när det gäller det organiserade dataskyddsarbetet starkt centrerat kring ISAM som, bland mycket annat, även ska vägleda hela förvaltningen när det gäller dataskyddsfrågor enligt Lokal anvisning för informationssäkerhet. GDPR är komplex och det krävs en hög samverkan inom en verksamhet för att få till stånd ett fungerande dataskyddsarbete. Detta medför att det inte är möjligt för ISAM att axla samtliga krav som GDPR ställer upp. Inte heller stadsdelsförvaltningens chefer kan klara av att axla kraven utan kunnig vägledning inom dataskydd. Dataskyddsombudet DSO ska inte utföra det operativa arbetet.

Då ISAM har fullt upp med att hantera sina huvuduppgifter inom informationssäkerhetsarbetet och hantera registerförteckningen så finns det lite utrymme för att hantera övriga dataskyddsfrågor. När det gäller de krav som GDPR ställer upp och som inte går i linje med informationssäkerhetsprocesserna krävs det en förstärkning.

Även om det finns andra personer inom förvaltningens verksamhet som har uppgifter som rör dataskyddsarbetet saknas det någon som kan vara en kunskapskälla och pådrivare med huvudsaklig inriktning mot dataskydd i det löpande operativa arbetet. Dataskyddsarbete kräver ett omfattande förankringsarbete dels när det gäller att uppdatera alla rutiner och dokument dels när det gäller att hålla ihop alla delar av processen dels när det gäller att minska personberoendet i arbetet med dataskyddsfrågorna. Dessutom är ISAM upptagen med informationsklassningar där det finns en massiv skuld.

Organisationen av dataskyddsarbetet inom stadsdelsförvaltningen som ska kunna klara av samtliga krav som ställs enligt GDPR är inte hållbart varför jag föreslår att det genomförs en organisatorisk förstärkning av dataskyddsarbetet inom stadsdelsförvaltningen enligt följande:

Förvaltningen måste ges i uppdrag att organisera ett löpande dataskyddsarbete som klarar av att hantera de krav som GDPR ställer på en personuppgiftsansvarig. Detta kräver bland annat att en erfaren dataskyddssamordnare utses med övergripande ansvar för det operativa dataskyddsarbetet inom stadsdelsförvaltningen. Vidare krävs att ledningsgrupp, ansvariga chefer och utsedda dataskyddsambassadörer får en omfattande dataskyddsutbildning för att kunna ta ansvar för det löpande dataskyddsarbetet som verksamheten kräver. Förvaltningsledningen bör innan en dataskyddssamordnare är på plats ta ansvar för att dataskyddsarbetet även fungerar inom staden så att kontrollen kan stärkas även om behandlingsystem och tjänster inte finns inom stadsdelsförvaltningen.

Vidare krävs ett omtag när det gäller styrande dokument och rutiner så att dataskyddsarbetet kan utvecklas av dataskyddssamordnaren i samverkan med övriga nyckelpersoner, ISAM och DSO.

8. Information till den registrerade såväl internt som externt

Bakgrund och syfte

Informationskraven enligt GDPR kring personuppgiftsbehandlingar är omfattande (art 12-14 GDPR) och är en viktig fråga kring transparensen i dataskyddsarbetet.

Informationskraven gäller alla typer av behandlingar hos en personuppgiftsansvarig. Informationen ska vara tydlig och begriplig så att det är tydligt vilka uppgifter som används för vilket ändamål och enligt vilken grund för varje personuppgiftsbehandling som sker. Det ska även framgå vem informationen delas med och inte minst hur länge personuppgifterna sparas. Även användning av personuppgiftsbiträden ska framgå och om det förekommer att personuppgifter överförs till tredje länder, det vill säga utanför EU/EES.

Att lämna en tydlig utformad information till den registrerade är en förutsättning för att kunna behandla personuppgifterna överhuvudtaget (med få undantag).

Informationen ska vara klar och tydlig och ska tillhandahållas den registrerade i god tid före det att behandlingen sker exempelvis vid insamlandet av uppgifterna eller senast inom 30 dagar från insamlandet eller, om behandlingen sker dessförinnan, senast vid behandlingen.

Informationen ska även utförligt ta upp hur de registrerade kan ta tillvara sina rättigheter och möjlighet att klaga. Där ska även dataskyddsombudets kontaktuppgifter framgå.

Det finns en riktlinje som tagits fram på EU-nivå med utförliga anvisningar om hur informationen ska presenteras (Riktlinjer om öppenhet, WP260rev0.1) samt åtskilliga beslut och rättsfall inom EU som visar nivån på öppenheten.

Kontroller och iakttagelser gjord av dataskyddsombudet

Stadsdelsförvaltningen har inte tagit fram någon egen samlad information om de personuppgiftsbehandlingar som genomförs. Det gäller såväl personuppgiftsbehandlingar som sker i verksamheten som de behandlingar som rör interna förhållanden som omfattar främst de anställda bland annat IT-användning, HR, Ekonomi säkerhet mm. Det finns viss information som framgår i olika processer men informationskraven enligt GDPR är höga och det är viktigt att kunna se över och hålla informationen uppdaterad utifrån de behandlingar som pågår inom verksamheten och internt. Tillgång till en lättillgänglig samlad information är central i dataskyddsarbetet.

Den information som finns centralt framtagen av staden, som man idag lutar sig emot, är inte tillräcklig för att uppfylla GDPRs alla krav kring information.

Informationskraven gäller även för behandlingar som sker internt hos en personuppgiftsansvarig. Även här är det stadens information som vi använder med några undantag.

Inom HR-området förekommer en stor mängd behandlingar som rör dels anställda dels känsliga eller i vart fall integritetskänsliga uppgifter även det i stor omfattning. Generellt är informationen om behandlingar som sker inom staden och även inom stadsdelsnämndens verksamhet bristfällig och inte samlad på det sätt som är nödvändigt.

Då vi är beroende av stadens information har vi begränsade möjligheter att själva utforma informationen efter den verksamhet som vi faktiskt bedriver inom stadsdelsförvaltningen.

Dataskyddsombudets bedömning samt rekommendationer

Att lämna tydlig informationen om alla personuppgiftsbehandlingar är en grundläggande förutsättning för all behandling av personuppgifter såväl internt som externt. Det behöver tas fram en extern information som avser de behandlingar som vi inom stadsdelsförvaltningen ansvara för. Den är nödvändig för att vi ska kunna ha egen kontroll över informationen när det sker förändringar i våra behandlingar av personuppgifter. Den kan på samma sätt som information från andra förvaltningar placeras på stadens öppna hemsida. Vidare behöver det tas fram en intern information som rör all personuppgiftsbehandling som sker med personalens personuppgifter. Denna information ska finnas tillgänglig på stadsdelsförvaltningens interna hemsida.

Informationen ska även utförligt ta upp hur de registrerade kan ta tillvara sina rättigheter och möjlighet att klaga. Där ska även dataskyddsombudets kontaktuppgifter framgå.

Det är vidare viktigt att det finns någon utpekad ansvarig för informationen. Även här kan den föreslagna ansvarige dataskyddssamordnaren träda in.

9. Stadengemensamma tjänster och utveckling

Bakgrund och syfte

Stadsdelsnämnden/förvaltningen kan inte enbart ta ansvar för dataskyddsarbete som sker inom den egna förvaltningen utan har ansvar för ”våra” personuppgifter även när de behandlas av utomstående parter och i projekt inom staden och i de centrala systemen som tillhandahålls av staden eller har upphandlats från någon extern tjänsteleverantör (exempelvis Miljödata). En personuppgiftsansvarig ska organisera sitt dataskyddsarbete så att man kan upptäcka och hantera de risker som verksamheten medför och vidta de säkerhetsarrangemang som är nödvändiga för att skydda och behålla kontrollen över personuppgifterna. Det kan bland annat innebära att man kontrollerar tjänsteleverantörer och ser över de säkerhetsarrangemang som finns på plats enligt de överenskommelser som man kommit överens med olika typer av aktörer om.

Kontroller och iakttagelser gjord av dataskyddsombudet

Det är vanligt förekommande att dataskyddsarbetet är eftersatt i centrala utvecklingsprojekt och att nödvändig informationsklassning, tröskelanalyser och konsekvensbedömningar inte har genomförts trots att projekten pågått länge och kanske till och med gått in i en införandefas. Detta är mycket oroande och är ytterligare tecken på att dataskyddsarbetet även inom staden är eftersatt vilket påverkar säkerheten och kontrollen över bland annat ”våra” personuppgifter. I centrala projekt borde det löpande dataskyddsarbetet tas om hand av en operativ dataskyddsorganisation. Tyvärr saknas detta varför det blir dataskyddsombuden som är utsedda av respektive stadsdelsförvaltning/förvaltning som får ta det ansvaret trots att det inte ska ingå i dataskyddsombudets åtaganden. Brister i dataskyddsarbetet är mer regel än undantag. Detta är ett problem då vi som stadsdelsnämnd/förvaltning är ansvariga tillsammans med övriga förvaltningar för vad kommunen som helhet ska ta ansvar för gällande dataskyddsarbetet. Vi måste kunna kontrollera att dataskyddsarbetet sköts även i centrala projekt för att vi ska kunna påvisa att vi har kon troll över och har vidtagit tillräckliga säkerhetsåtgärder för när andra förvaltningar hanterar ”våra” personuppgifter.

Dataskyddsombudets bedömning samt rekommendationer

Stadsdelsförvaltningen bör ges i uppdrag att tillsammans med övriga stadsdelsförvaltningar tillsammans verka för att det sker en tydlig ansvarsuppdelningen inom staden när det gäller

personuppgiftsbehandlingar som sker i centrala IT-system och hos andra förvaltningar inom staden. Denna ansvarsuppdelning bör formaliseras genom en tydlig överenskommelse så att alla dataskyddsfrågor kan tas om hand i gemensamma system och i alla utvecklingsprojekt som sker inom staden inte minst vid den pågående digitaliseringen. En sådan ansvarsfördelning måste göras tillgänglig på stadens externa hemsida. Det är en operativ dataskyddsorganisation inom staden som ska sköta dessa dataskyddsfrågor.

En överenskommelse är viktig så att vi i stadsdelsnämnden/förvaltningen kan ta ansvar för ”vår” information även då den hanteras av stadens andra förvaltningar och i olika utvecklingsprojekt. Innan en sådan överenskommelse kan komma på plats måste förvaltningen bevaka centrala utvecklingsprojekt som kan komma att, likt projektet kring Miljödata, använda ”vår” information i projekten. Vi måste då kunna klara av att ställa krav för att skydda ”vår” information och se till att dataskyddsarbetet även i övrigt tas om hand.

Bilaga 2 – Omvärldsbevakning i korthet

Omvärldsbevakning

Resultatet av dataskyddsombudets omvärldsbevakning

IMY:s granskningar utifrån Miljödata-läckan

Integritetsskyddsmyndighet (IMY) har inlett granskningar med anledning av IT-angreppet mot Miljödata och de personuppgifter som då läckte. Granskningarna gäller företaget Miljödata samt två kommuner och en region som använt företagets tjänster.

Tillsyn har inletts mot Miljödata i Karlskrona AB, Göteborgs stad, Region Västmanland och Älmhults kommun.

Följande frågor har ställts till Göteborgs Stad:

Våra frågor

Personuppgiftsansvar

1. Är ni personuppgiftsansvarig för den personuppgiftsbehandling som skett i Miljödatas system avseende personuppgifter tillhörande anställda eller tidigare anställda hos Göteborgs kommun? Om nej vem/vilka är personuppgiftsansvarig inom kommunen för behandlingen? Lista ev. förvaltningar som är personuppgiftsansvariga efter storleksordning (utifrån antal registrerade vars personuppgifter har behandlats).

2. Har ni anlitat Miljödata som personuppgiftsbiträde? När anlitade ni Miljödata? Bifoga personuppgiftsbiträdesavtalet till ert svar till IMY.

3. Redogör för hur ansvaret är reglerat för att bedöma och vidta lämpliga säkerhetsåtgärder mellan den som är personuppgiftsansvarig och personuppgiftsbiträde för behandlingen i Miljödatas system.

Personuppgifter

4. Hur omfattande är er behandling av personuppgifter i Miljödatas system? Beskriv antal registrerade och hur länge personuppgifterna behandlas i systemet.

5. Vilka slags personuppgifter har ni behandlat i Miljödatas system?

6. Har ni behandlat skyddade personuppgifter i Miljödatas system?

7. Har ni behandlat barns personuppgifter i Miljödatas system?

….

Bara för att tillsyn inte har öppnats mot Stockholms Stad i detta läge innebär det inte att denna tillsynsaktivitet inte kan komma att omfatta oss. Vi bör funder över hur vi kan svara på de frågor som Göteborg Stad fått ovan.

Något om IMYs arbete med tillsynsplaner mm.

Imy arbetar med tillsynsplaner som sträcker sig över flera år och den senaste planen omfattade åren 2022-2025 vilket medför att det i början av 2026 kommer komma en ny inriktning som kommer sträcka sig flera år framåt.

Jag vill här även visa på den målbild som gällt enligt den senaste planen.

Målbild 2025

I vår målbild 2025 konkretiseras visionen på några års sikt.

Vår målbild 2025 är att personlig integritet och dataskydd ges ett tydligt fokus på alla nivåer i samhället.

2025 vill vi att

- enskilda individer har god kunskap om sina rättigheter
- privata och offentliga verksamheter arbetar mer systematiskt med dataskydd och driver en integritetsvänlig digitalisering
- innovation och utveckling av teknik och tjänster sker på ett sätt som värnar den personliga integriteten
- Sverige har en tydlig integritetsskyddspolitik som bidrar till en hållbar digitalisering och
- IMY är en ännu mer attraktiv arbetsgivare.

För att nå målbilden att personlig integritet och dataskydd ges ett tydligt fokus på alla nivåer i samhället ska IMY

- ge stöd till enskilda individer genom att ha bra kunskapsstöd på vår webbplats och utreda klagomål när enskilda upplever att deras personuppgifter behandlas felaktigt.
- underlätta för privata och offentliga verksamheter genom att ta tydlig ställning i rättsliga frågor och bidra till att utveckla praxis. Vårt mål är att vara en kunskapsbank där det är lätt att hitta relevant information, så att det blir enklare att följa dataskyddsreglerna. Vi ska genomföra fler tillsynsärenden än tidigare och ha effektiva processer – därmed bidrar vi till att upprätthålla förtroendet för regelverket.
- bidra till hållbar innovation och utveckling genom att ha en god förmåga att följa och analysera teknikutvecklingen och ge vägledning och stöd till innovationsaktörer.
- bidra till utvecklingen av en tydlig integritetsskyddspolitik genom att aktivt delta i samhällsdebatten, ge vägledning och stöd till regering och riksdag och vara en konstruktiv remissinstans.
- vara en attraktiv arbetsgivare genom att erbjuda utvecklingsmöjligheter, ett tillitsbaserat ledarskap och en flexibel, trevlig och hjälpsam arbetsmiljö.

I samband med IMYs DSO-konferens på Nobeldagen 2025 informerade IMYs generaldirektör att IMY kommer att genomföra vissa organisationsförändringar där det bland annat ska bildas en enhet som ska ha ökat fokus kring klagomål och genomföra fler tillsyner, särskilt planenliga sådana.

Intressant dom om förhållandet mellan dataskydd och allmän handling.

Högsta förvaltningsdomstolen (HFD) prövar rätten till tillgång (art 15) till personuppgifter i uppgifter som inte är allmänna (dom meddelad den 18 juni 2025)

- En registrerad har begärt att få ta del av handlingar hos Kammarrätten i Jönköping.
    - Begäran avsåg handlingar i flera mål om rätt att ta del av allmänna handlingar samt ett e-postmeddelande som skickats inom Kammarrätten.
    - Kammarrätten avslog begäran, ansåg inte att det var allmänna handlingar
    - HFD anser att rätten till tillgång även gäller för personuppgifter i handlingar som inte är allmänna
    - Kammarrätten hade inte fog för att avslå den registrerades begäran

Slutsats:

Det är inte alltid enkelt att hantera flera regelverk samtidigt.

IMY har publicerat tre nya filmer

IMY har publicerat tre nya kunskapsfilmer om GDPR – nu finns totalt 11 stycken. Dessa tre nya kunskapsfilmer handlar om personuppgiftsincidenter, informationssäkerhet och konsekvensbedömningar. De är till för att öka kunskapen på ett enkelt och lättillgängligt sätt.

Tillhörande quiz finns till respektive film.

Dessa filmer som är ca 10 minuter långa ger en bra grundförståelse för vad GDPR innehåller och borde vara en bra väg in i ämnet för dem som ska ta lite större ansvar för dataskyddsfrågorna. De är sannolikt bättre än de fortsättningsutbildningar som finns inom staden. Stadens fördjupningsutbildningar förutsätter att man redan kan grunderna i dataskydd och förstår regelverket.