Stockholms stad

GDPR Årsrapport

År 2024

Fastighetsnämnden

GDPR årsrapport 2024
December 2024

Dnr: YYYY
Utgivningsdatum: 2024-12-27
Kontaktperson: Christian Sandell

1. Bakgrund

Dataskyddsförordningen (nedan GDPR) trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen är att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. GDPR syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna inom EU.

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 och/eller biträde enligt GDPR.

I avsnittet ”Ansvar enligt GDPR” nedan anges kortfattat vilket ansvarsskyldighet som gäller för personuppgiftsansvariga respektive personuppgiftsbiträde enligt GDPR (8.2). Det är detta ansvar som jag som dataskyddsombud (DSO) utgår ifrån när jag bedömer regelefterlevnadsrisker till följd av brister i dataskyddsarbetet i denna rapport.

Som DSO har jag som huvudsaklig uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad. Jag ska vidare 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 Jag ska vidare rapportera status för dataskyddsarbetet direkt till högsta förvaltningsnivå, vilket görs genom denna årsrapport.

I årsrapporten redogör jag som DSO för de granskningar och andra observationer som jag 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.

Innehåll

2. Sammanfattning

2.1 De två viktigaste åtgärderna enligt DSO

2.1.1 Grundläggande översyn av förutsättningarna för ett systematiskt hållbart dataskyddsarbete i löpande förvaltning

Förutsättningarna att kunna axla samtliga krav som ställs på oss enligt GDPR är inte hållbart varför jag föreslår att det genomförs en organisatorisk förstärkning av dataskyddsarbetet.

Det behöver utses dataskyddsambassadörer på de avdelningar där det förekommer behandling av känsliga personuppgifter. Vidare bör dataskyddssamordnaren få ansvar att utveckla dataskydds-arbetet inom kontoret med hjälp av de utsedda ambassadörerna. Dataskyddssamordnaren bör få utbildning i GDPR och kringliggande lagstiftning och riktlinjer från EU mm för att kunna utveckla dataskyddsarbetet i samverkan med DSO. Dataskyddssamordnaren måste ges tillfälle och resurser att återuppväcka rutiner och dokument och inte minst få registerförteckningen i ordning och starta arbetet med riskanalys och konsekvensbedömningar så att kontoret återtar kontrollen över personuppgiftsbehandlingarna. Vid en organisationsförändring kommer behovet även av DSOs tjänster att öka inledningsvis varför även den rollen kan kräva mer än dagens 20 % av en heltid initialt.

De chefer i verksamheten som ansvarar för behandlingarna med högre risk bör även få utbildning i dataskyddsfrågor.

Ledningen bör slutligen informeras om de krav som ställs på kontoret när det gäller ett fungerande dataskyddsarbete. Ledningen bör vidare vara aktiv i sin roll som informationsägare inom Staden för att få till stånd en bättre informationsdelning med alla objektägare för staden-gemensamma IT-tjänster som hanterar information som kontoret ansvarar för så att skyddsnivån är tillräcklig för kontorets behandlingar och kan bibehållas över tid.

2.1.2 Grundlig översyn av intern och extern information om personuppgiftsbehandlingar

GDPRs krav på transparens (art. 12-14) är omfattande och den externa informationen om personuppgiftsbehandlingarna har inte

stämts av mot de behandlingar som sker i verksamheten på flera år.
När det gäller transparensen över de behandlingar som sker internt inom Staden och som gäller de egna anställda (och konsulter) är bristerna omfattande. Här krävs det att personuppgifts-behandlingarna kartläggs och att intern information tas fram. Informationen föreslås publiceras på intranätet på motsvarande sätt som den externa informationen.

2.2 Översiktlig bedömd status för olika rapporteringsområden

Rapporteringsområde		Mindre	Omfattande	Allvarlig
Obligatoriska				
Registerförteckning			x	
Styrdokument			x	
Informationsklassning (Organisatoriska och tekniska åtgärder)		x		
Konsekvensbedömning		x		
Individens rättigheter	x			
Personuppgiftsincidenter		x		
Övriga observationer				
Ansvarsskyldigheten			x	
Information till registrerad extern			x	
Information till registrerad intern			x	
Stadengemensamma tjänster			x	
DSO			x	

(För specificering se respektive avsnitt)

Bedömningsmall för dataskyddsrisker:

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3. Presentation av DSO och arbetssätt

Mitt namn är Christian Sandell och jag är dataskyddsombud inom fastighetskontoret (20% av heltid) sedan mitten av september i år vilket medför att jag haft begränsad tid för att på djupet lära känna alla delar av dataskyddsarbetet som sker inom kontoret och inom Staden. Jag har expertkunskaper inom dataskyddsförordningen (GDPR) och har sedan ikraftträdandet i maj 2018 arbetat med dataskyddsfrågor på heltid som dataskyddsombud och som dataskyddsansvarig främst inom privat sektor.

För mig handlar dataskyddsarbete om att visa respekt för de mänskor vars personuppgifter vi samlar in och hanterar för olika syften. GDPR ställer höga krav vilket kräver en nära samverkan mellan olika funktioner i en verksamhet som IT, juridik, informationssäkerhet och dataskydd.

När vi använder besökandes, kunders 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 fri- och rättigheter inklusive skyddet av personuppgifter. Vi ska informera kunder 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 kontoret och inom Staden. 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 har försökt sammanställa ansvar och roller inom Staden i ett avslutande kapitel (8.1) nedan. Huvudansvaret för dataskyddsarbetet har lagts på respektive nämnd inom Staden.

4. Obligatoriska rapporteringsområden

I årsrapporten kommer de sex obligatoriska rapporteringsområden att redovisas även om de borde ha justerats över tid då dataskyddsarbetet är en pågående process där bedömnings-kriterierna måste justeras löpande i takt med att arbetet med dataskyddsfrågorna utvecklas inom en verksamhet och där verksamheten mognar i sin dataskyddsförmåga.

De obligatoriska rapporteringsområdena är registerförteckning, styrdokument, informationsklassning (som en del av tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar), konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter. Dessa rapporteringsområden har varit samma sedan de infördes.

Nedan redogörs för kontorets status och DSO:s slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:s genomförda uppföljning och inledande granskning.

Som ett led i uppföljningen av de obligatoriska delarna har verksamheten fått svara på ett antal frågor som DSO skickade ut (se bilaga 1). De svar som har lämnats på dessa frågor av verksamheten har beaktats i nedanstående bedömningen av respektive område.

4.1 Registerförteckning

4.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	67
Har nödvändiga uppdateringar gjorts?	Arbete pågår med att uppdatera ansvariga. Övrigt Nej
Bedöms registerförteckningen vara fullständig?	Även om flertalet behandlingar är upptagna är informationen ofullständig.
Har verksamheten lämpliga rutiner för registerföring?	Inga ändring de senaste åren. Antal samma. Tveksamt.

4.1.2 Syfte

Förteckning på behandlingar, även kallad behandlingsregistret eller registerförteckning, är ett direkt lagkravkrav enligt GDPR. Kravet innebär att samtliga behandlingar av personuppgifter ska kartläggas i ett behandlingsregister. Informationen i behandlingsregistret ska hållas uppdaterad, aktuell och komplett och granskas av DSO. Syftet med detta avsnitt är att granska kontorets registerförteckning.

4.1.3 Resultatet av genomgången

Registerförteckningen är upprättad i Draftit och följer såvitt kan bedömas den standardmall som tillhandahålls av systemet.
Av registret framgår att det på flera frågor anges ”vet ej” exempelvis när det gäller tredjelandsöverföringar. Det är vidare oklart om information lämnats på riktigt vis gällande flera av behandlingarna. Det finns en behandling som kräver vidare utredning (Kontroll och övervakning av e-post och internet) där det finns många oklarheter. Även uppgift om dataskyddsombud är felaktig. Många registerpunkter är sammansatta så att det är svårt att få en överblick över behandlingarna som ingår. De flesta registreringar är gjorda för många år sedan och det finns områden som rör egen personal och även övervakning som kan behöva ses över grundligt. Även de behandlingar som är markerade med högre risk bör genomgå en fullständig revision.
Kamerabevakningen av Tekniska Nämndhuset är inte med i förteckningen.

4.1.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
x	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

4.1.5 DSO ger råd och rekommendationer till PUA

Det finns skäl att göra en grundlig översyn av innehållet i registerförteckningen för att få den att fungera som den överblick över behandlingarna som det är tänkt. En registerförteckning ska vara så fullständig så att den kan lämnas ut till tillsynsmyndigheten IMY vid begäran. Översynen bör initialt

omfatta de registreringar som är angivna med hög risk, samtliga registreringar som kan innehålla känsliga uppgifter och alla registerpunkter som rör HR-avdelningen. Kamerabevakning bör finnas med som registerpost.

4.2 Styrdokument

4.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Det saknas Lokal anvisning för informationssäkerhet
Håller innehållet i de existerande dokumenten lämplig kvalitet?	I stort gällande dataskydd
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	De centrala dokumenten saknar väsentliga delar när det gäller dataskyddsarbetet
Är dokumenten uppdaterade?	Delegationsordningen är uppdaterad.
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Såvitt kan bedömas när det gäller nyare styrdokument

4.2.2 Syfte

Styrdokument ska finnas nedtecknade, beslutade och kommunicerade. Genom styrdokument kommuniceras till medarbetarna vad som förväntas av dem samt information om regler, ramar och förutsättningar och stöd för att upprätthålla kunskapen över tid och tillämpa den på ett konsekvent sätt. Syftet med detta avsnitt är att granska kontorets styrdokument inom dataskydd.

4.2.3 Resultatet av genomgången

Det kan först konstateras att det finns styrande dokument som efter att de har antagits (2019-2020) inte har vare sig efterlevts eller uppdaterats. Dessa finns i samarbetsytan för GDPR. Det gäller bland annat ett årshjul för DGPR-arbete och en instruktion för DSO som inte går att få fram då länken till huvuddokumentet är borta.
När det gäller nyare styrdokument så är kontorets verksamhet styrt av stadens centrala styrdokument. Den lokala anvisningen för informationssäkerhet är under framtagande enligt uppgifter i

tertialrapporteringen men går inte att återfinna på samarbetsytan. Ledningens genomgång (inför 2024) är en början för verksamheten att bli mer aktiv i den regelflora som styr delar av verksamheten och som förväntas öka med nya EU-regelverk. Ledningens genomgång behöver även beröra dataskyddsarbetet då det ingår i informationssäkerhetsarbetet.

4.2.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
x	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

4.2.5 DSO ger råd och rekommendationer till PUA

Det finns äldre styrdokument på samarbetsytan som bör revideras för att bedöma om de ska uppdateras eller utmönstras. Det är angeläget att det viktiga lokala styrdokumentet Lokal anvisningen för informationssäkerhet beslutas och att det även kommer omfatta en reglering av ansvaret för dataskyddsarbetet med beaktande av de krav som ställs upp i GDPR (se avsnitt 8.2). Ledningens genomgång behöver vidare utökas med inriktning på att dataskydd är en del av informationssäkerhetsarbetet.

4.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

4.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	Klassning verkar ske av informationsmängder som används i olika processer. Huvuddelen av dessa är klassade
Är klassade personuppgiftsbehandlingar aktuella?	Svårt att bedöma då registret är ofullständigt och såvitt jag kan se inte är kopplat till klassningarna.

4.3.2 Syfte

För att kunna skydda information som även omfattar personuppgifter med rätt slags skydd så ska verksamheten informationsklassa sin information. Informationsklassning av information och av system är viktiga byggstenar för att kunna bedöma om personuppgiftsbehandlingen är skyddad på rätt sätt. Syftet med detta avsnitt är att bedöma rutinerna kring informationsklassning med hänsyn till de personuppgiftsbehandlingar som hanteras inom kontoret.

4.3.3 Resultatet av genomgången

Kontoret följer de centrala dokumenten Handbok för informationsklassning. Informationsägaren ska initiera informationsklassning. Även om jag haft begränsade möjligheter att följa upp så ska alla utom 4 behandlingar vara klassade. Någon informationsklassning ska inte vara genomförd under 2024. Det finns ingen plan för löpande riskbedömning vid ändrade förhållanden.

4.3.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
x	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

4.3.5 DSO ger råd och rekommendationer till PUA

Det bör finnas rutin för att med visst mellanrum ompröva informationsklassningen så att säkerhetsskyddet ska kunna anpassas så att personuppgifterna skyddas på rätt nivå.

4.4 Konsekvensbedömningar

4.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Enligt verksamheten har konsekvensbedömningar gjorts
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Ingen konsekvensbedömning är genomförd under 2024
Är de genomförda bedömningarna aktuella?	Bedömningarna är i huvudsak från 2019

4.4.2 Syfte

En konsekvensbedömning är nödvändig när det bedöms att en behandling kan innebära en hög risk för registrerades friheter och rättigheter. Syftet med att göra konsekvensbedömningar är att förebygga risker för att skydda de registrerade och att efterleva GDPR. En konsekvensbedömning är en bedömning av de konsekvenser som kan uppstå när man behandlar personuppgifter. I bedömningen tar man ställning till om risken är proportionerlig i förhållande till ändamålet med behandlingen av uppgifterna. Visar det sig att risken är för hög för att motivera ändamålet kan bedömningen resultera i att det inte går att genomföra behandlingen, alternativt ta fram skyddsåtgärder för att sänka risken. Dessa skyddsåtgärder kan vara tekniska eller organisatoriska

För att få en uppfattning om en personuppgiftsbehandling innebär en hög risk ska normalt alla personuppgiftsbehandlingar genomgå en så kallas ”tröskelanalys”. Vid tröskelanalysen bedöms om kriterier för hög risk enligt GDPR (art. 35) och enligt IMYs riktlinjer är aktuella. Om så är fallet så är det nödvändigt att genomföra en konsekvensbedömning.

Syftet med detta avsnitt är att granska kontorets rutin för konsekvensbedömningar samt att ge rekommendationer kring det fortsatta arbetet.

4.4.3 Resultatet av genomgången

Det finns en rutin för riskanalys som innefattar den så kallade tröskelanalysen. Det finns även riskanalyser och

konsekvensbedömningar som genomförts 2019 i större omfattning.

4.4.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
x	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

4.4.5 DSO ger råd och rekommendationer till PUA

Då registerförteckningen behöver genomgås bör även tröskelanalyser genomföras i samband med den genomgången för att förnya behovet av konsekvensbedömningar. Det bör införas en rutin för att löpande revidera gjorda konsekvensbedömningar så att skyddsnivåer kan upprätthållas.

4.5 Individens rättigheter

4.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	1 gällande registerutdrag
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	1

4.5.2 Syfte

Individens rättigheter regleras i flera artiklar i GDPR. Några rättigheter som kan nämnas är den registrerade rätt att begära och få registerutdrag, rätt till rättelse samt rätt till radering.
När en begäran kommit in från en registrerad ska det finnas rutiner så att begäran kan hanteras av verksamheten inom 30 dagar.

Syftet med detta avsnitt är att granska kontorets dokumentation och rutiner gällande individens rättigheter samt att ge rekommendationer kring det fortsatta arbetet.

4.5.3 Resultat av genomgången

Det finns framtagna rutiner och utsedda personer för hantering av begäran från registrerad både vad det gäller registerutdrag och annan begäran. Då rutiner och andra underlag tagits fram 2019-2020 så anges datainspektionen i materialet. Rutinen har använts för enstaka registerutdrag och fungerar även om den är helt manuell i sammanställningsfasen.

4.5.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
x	Inga brister av nämnvärd betydelse identifierade

4.5.5 DSO ger råd och rekommendationer till PUA

Rutiner och material behöver gås igenom och förnyas. Rutinen för ett registerutdrag är omfattande och innebär manuell hantering. En större belastning skulle kunna innebära hög belastning för berörd personal att klara tidsgränserna. Mot bakgrund av kontorets verksamhet är risken mindre men bör beaktas.

4.6 Personuppgiftsincidenter

4.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur många personuppgiftsincidenter har dokumenterats?	Inga
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Inga
Hur många av incidenterna har rapporterats i tid till IMY?	_

4.6.2 Syfte

Att identifiera och hantera personuppgiftsincidenter är ett direkt krav i GDPR. Det är även viktigt att aktivt arbeta med att förebygga personuppgiftsincidenter för att spara tid och resurser samt för att bygga en riskmedveten säkerhetskultur inom kontoret.

En personuppgiftsincident ska normalt anmälas till IMY inom 72 timmar. Anmälan till IMY behöver inte ske om den personuppgiftsansvarige kan visa att det är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter.

Syftet med detta avsnitt är att granska kontorets rutiner och processer gällande personuppgiftsincidenter samt att ge rekommendationer kring det fortsatta arbetet.

4.6.3 Resultat av genomgången

Det finns en rutin kring hantering av personuppgiftsincidenter. Rutinen är som övrigt material framtagen 2019 och innehåller datainspektionen som tillsynsmyndighet. Vidare är den nya E-tjänsten hos IMY inte beaktad utan allt utgår från den manuella hanteringen som gällde vid tiden för rutinens framtagande.

4.6.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
x	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

4.6.5 DSO ger råd och rekommendationer till PUA

Rutinen behöver revideras och DSO:s roll behöver uppdateras. Ansvaret för anmälan till IMY bör ligga på verksamheten även om DSO bör involveras i samband med utredningen av incidenten. Dokumentationen av personuppgiftsincidenter bör ses över.

5. Gjorda observationer under året

1. Ansvarsskyldigheten
2. Information till den registrerade externt
3. Information till den registrerade internt
4. Stadengemensamma tjänster
5. Information om och kontaktuppgifter till DSO

Som nytt dataskyddsombud har jag haft anledning att ta reda på hur dataskyddsarbetet ser ut inom kontoret och inom Staden. Jag har gått in på Stadens externa sidor och observerat hur information har presenterats för en besökare. Jag har även gått in på de interna sidorna och gjort motsvarande observationer där hur dataskyddsfrågor hanterats och vilken information som funnits där. Jag har även gjort observationer på lokala samarbetsytor och i samband med olika möten och samtal med personer inom Staden och på kontoret.

Vid dessa genomgångar har jag stött på olika frågeställningar där jag har känt att det finns brister och oklarheter som behöver hanteras på olika sätt men att det av olika skäl inte funnits tid för att ta hand om varje enskild brist direkt. Även positiva observationer har gjorts. Då jag har en ambition att vilja se ett gott dataskyddsarbete inom kontoret (men även inom de andra förvaltningar där jag är DSO) har jag valt att i denna årsrapport flagga upp att det finns flera områden (utöver de obligatoriska) där det finns en tydlig förbättringspotential så att nämnden, ledningen och dataskyddsorganisationen inom kontoret kan ta frågorna vidare.

5.1 Ansvarsskyldigheten

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
x	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

5.1.1 Grundläggande krav enligt GDPR

Enligt GDPR (art 5:2) har den personuppgiftsansvarige ett ansvar för att alla grundläggande dataskyddsprinciper efterlevs gällande all personuppgiftsbehandling i en verksamhet. Den person-

uppgiftsansvarige 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.

5.1.2 Observation

Som personuppgiftsansvarig men (även som biträde) 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 hamna i strid med vad som anses som bra informationssäkerhet.

Dataskyddsarbetet inom Staden har efter att införandeprojektet avslutades 2019 formats lokalt inom respektive förvaltning vilket har medfört att delar av dataskyddsarbetet fungerar men att andra delar har försummats eller inte har beaktats. För kontorets del är detta tydligt där huvuddelen av dataskyddsarbetet utfördes under 2019-2020 för att därefter tappa farten. Registerförteckningen är fortfarande inte i ordning och ansvariga för informationen har inte kunskapen och förståelsen för vad ett systematiskt dataskyddsarbete kräver.
Kontorets organiserade dataskyddsarbete är uppbyggt kring några få nyckelpersoner vilket har gjort och gör det sårbart och utan styrning. Styrdokument och rutiner är inte uppdaterade och har inte förändrats trots att kraven på ett systematiskt dataskydds-arbete har ökat genom alla beslut och domslut inom EU.

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 både 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 t.ex. inventering och upprättande av registerförteckning.”(se sid 5 i Stadsrevisions rapport nr 5, 2019) så gick utvecklingen åt ett annat håll. När det gäller kontoret så finns det fortfarande delar i rutiner och anvisningar som pekar ut DSO som drivande i olika delar av dataskyddsarbetet. Även det faktum att ansvaret för dataskyddsarbetet i de centrala styrdokumenten har landat i att det är informationsägarna (ofta verksamhetens chefer) som har krav på sig att leva upp till kraven i GDPR har gjort dataskyddsarbetet lidande. . 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. För att inte glömma alla objektägare såväl i den egna verksamheten som inom Staden. Det som saknats är någon som kunnat ansvarar för att hålla ihop alla delar och se till att delarna hanteras i rätt ordning i de olika processerna. En dataskyddsansvarig med hög kunskap inom GDPR och med genomförandeförmåga så att brister och behov kan omhändertas löpande.

Detta har gjort att det idag finns betydande brister i organisationen av kontorets dataskyddsarbete. 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 kontoret.

I min bedömning utgår jag från de krav som GDPR ställer upp på en personuppgiftsansvarig (se avsnitt 8.2) varför jag drar slutsatsen att verksamheten inte är organiserad så att den 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.

Kontorets verksamhet när det gäller olika typer av personuppgifts behandlingar är begränsad men det finns områden som kräver uppmärksamhet. Det gäller bland annat hela HR området och de delar som rör olika typer av övervakning digitalt eller via kamera. Sker det behandling av känsliga uppgifter är även dessa behandlingar av intresse.

För kontorets del är situationen när det gäller det organiserade dataskyddsarbetet fördelat mellan ISAM och en dataskyddssamordnare som båda även har andra arbetsuppgifter. Även andra personer inom kontorets verksamheter har uppgifter som rör dataskyddsarbetet men det saknas någon som kln vara en kunskapskälla och pådrivare med huvudsaklig inriktning mot

dataskydd utöver min roll som DSO. Skälet till detta är att det krävs ett omfattande förankringsarbete dels när det gäller att uppdatera alla rutiner och dokument dels när det gäller att minska personberoendet i arbetet med dataskyddsfrågorna. Det krävs någon som i samverkan med DSO kan utveckla utsedda dataskyddsinriktade personer inom respektive verksamhetsområde så att det löpande systematiska dataskyddsarbetet kan komma igång och hållas vid liv. Om man beaktar att även andra EU-regelverk kommer att kräva liknande lösningar så kan denna föreslagna organisationsförändring sannolikt komma att kunna återanvändas eller utökas med ytterligare uppgifter.

5.1.3 Råd och rekommendation

Förutsättningarna att kunna axla samtliga krav som ställs på oss enligt GDPR är inte hållbart varför jag föreslår att det genomförs en organisatorisk förstärkning av dataskyddsarbetet.

Det behöver utses dataskydds-ambassadörer på de avdelningar där det förekommer behandling av känsliga personuppgifter. Vidare bör dataskyddssamordnaren få ansvar att utveckla dataskyddsarbetet inom kontoret med hjälp av det utsedda ambassadörerna. Dataskyddssamordnaren bör få utbildning i GDPR och kringliggande lagstiftning och riktlinjer från EU mm för att kunna utveckla dataskyddsarbetet i samverkan med DSO. Dataskyddssamordnaren måste ges tillfälle och resurser att återuppväcka rutiner och dokument och inte minst få registret i ordning och starta arbetet med riskanalys och konsekvensbedömningar så att kontoret återtar kontrollen över behandlingarna.

Även en översyn och uppdatering av informationen om personuppgiftbehandlingarna behöver genomföras så att informationen är i enlighet med de krav som GDPR och praxis ställer upp såväl externt som internt.

Vid en organisationsförändring kommer behovet även av DSOs tjänster att öka inledningsvis varför även den rollen kan kräva mer än dagens 20 % av en heltid initialt.

De chefer i verksamheten som ansvarar för behandlingarna med högre risk bör även få utbildning i dataskyddsfrågor.

Även ledningen bör informeras om de krav som ställs på kontoret när det gäller ett fungerande dataskyddsarbete. Ledningen bör vidare vara aktiv i sin roll som informationsägare inom Staden för att få till stånd en bättre informationsdelning med alla objektägare för staden-gemensamma IT-tjänster som hanterar information som

kontoret ansvarar för så att skyddsnivån är tillräcklig och kan bibehållas över tid.

5.2 Information till den registrerade externt

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
x	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

5.2.1 Krav enligt GDPR

Informationskraven enligt GDPR kring personuppgifts-behandlingar är omfattande (art 12-14) 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 du vet vilka uppgifter som används för vilket ändamål och grund för respektive personuppgiftsbehandling. 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.

5.2.2 Observation

Kontorets framtagna information är bristfällig i de flesta delar vid jämförelse med lagstiftningen och riktlinjen. Inte heller den information som Kontoret hänvisar till (det vill säga stadens information) är tillfredsställande eller ens i linje med de krav som ställs på information till registrerade.

Bristerna består främst i att det är alltför generella skrivningar kring de olika behandlingarna och att det inte går att få veta vem som får ta del av de personuppgifter som lämnas efter behandling. Även de registrerades rättigheter är ofullständigt beskrivna. Det saknas även kontaktuppgifter till DSO. Den adress som är lämnad är en funktionsbrevlåda som flera medarbetare har tillgång till.

5.2.3 Råd och rekommendation

Informationstexten behöver ses över och omarbetas så att beskrivningen stämmer med behandlingarna som tagits med i registret och som även utförs inom kontorets verksamhet.

5.3 Information till den registrerade internt

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
x	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

5.3.1 Krav enligt GDPR

Informationskraven enligt GDPR kring personuppgifts-behandlingar är omfattande (art 12-14) 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 du vet vilka uppgifter som används för vilket ändamål och grund för respektive personuppgiftsbehandling. 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.

5.3.1 Observation

Informationskraven gäller även för behandlingar som sker internt hos en personuppgiftsansvarig.

När det gäller den interna informationen finns det brister. Det räcker inte med att information har lämnats vid något skede exempelvis vid en rekrytering. Det måste gå att ta del av den informationen även vid fortsatt anställning och en lämplig plats är på intranätet. Vid förändringar i olika typer av behandlingar inom HR så är det krav på att informationen ska lämnas till anställda innan behandlingen påbörjas. Om informationen ligger på intranätet är det lätt att hänvisa till den vid ändringar och uppdateringar.

Även här är det viktigt med tydlig informationen och att de olika behandlingarna av personuppgifter gällande anställda inklusive eventuell övervakning som sker digitalt och via kamera framgår tydligt.

5.3.2 Råd och rekommendation

Det är viktigt att även interna behandlingar informeras tydligt om på intranätet på samma sätt som är normalt gällande den externa hemsidan. Även förekomst av cookies och annan spårning internt är viktigt att informera om.
Informationen ska även utförligt ta upp hur de registrerade kan ta tillvara sina rättigheter och möjlighet att klaga. Där ska även dataskyddsombudets kontaktuppgifter framgå.

5.4 Stadengemensamma tjänster

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
x	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

5.4.1 Krav enligt GDPR

GDPR utgår ifrån att såväl personuppgiftsansvarig som biträde har organisatoriska och tekniska åtgärder på plats för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken för fysiska personers rättigheter och friheter vid all behandling (art. 32)

5.4.2 Observation

Inom staden har man delat upp ansvaret ur ett informationssäkerhetsperspektiv när det gäller olika typer av IT-tjänster även om de används av samtliga nämnder inom staden. Ur ett dataskyddsperspektiv ska varje förvaltning i egenskap av informationsägare, som vill bruka en IT-tjänst, göra nya riskbedömningar och konsekvensbedömningar utifrån den information som man avser att hantera i IT-Tjänsten. Detta förhållande är särskilt uttalat i centralt styrande dokument. Då tjänsterna oftast är upphandlade borde det finnas genomförd informationsklassning och framtagna upphandlingskrav och även ett gällande tjänsteavtal med SLA och personuppgiftsbiträdesavtal med instruktioner och krav på säkerhetsskydd. Även en processbeskrivning borde finnas tillgänglig.

I flera fall har det framkommit att det är svårt att som informationsägare få tillgång till dessa underlag som legat till grund för den ursprungliga anskaffningen av IT-tjänsten. Denna information borde finnas samlad hos objektägaren eller i objektstyrgruppen. Det borde även gälla för IT-tjänster som ligger externt.
Då det är objektägaren för IT-tjänsten som ansvarar för informationssäkerhetsarbetet som avser drift underhåll och utveckling av IT-tjänsten (Tillämpningsanvisning till stadens riktlinje för informationssäkerhet, 1.4.2) så bör det, trots att det inte är uttalat, ändå vara objektägaren som ansvarar för dataskyddsfrågorna som har samband med IT-tjänsten.

Problemen med delat ansvar i en fråga är att det ofta uppstår problem med att få information som är nödvändig för att med eget ansvar veta om information kan hanteras säkert i en IT-tjänst där det saknas underlag för att veta exempelvis hur tjänsten är utformat, var information hämtas ifrån och hur den processas, hur slutresultatet delas.

Även underleverantörer bör det finnas information om då det kan ha betydelse när det gäller tredjelandsöverföringar och annat.

Det är en återkommande fråga bland annat i Dataskyddssamverkansgruppen (GUG) att det är svårt att få fram nödvändiga underlag när det är dags för informationsägaren att genomföra sin riskanalys och konsekvensbedömning för att kunna bedöma om det går att använda IT-tjänsten för den personinformation man svarar för.

Under 2024 har inställningen inom Staden ändrats i detta avseende och så kallade normerande klassningar har påbörjats avseende gemensamma IT-tjänster. Avsikten är att även informations-ägarnas krav ska beaktas i samband med riskbedömning och klassning. Även om det inte är uttalat i styrdokumenten bör konsekvensbedömning sannolikt ingå i förfarandet.

En stor del av stadens behandlingar särskilt när det gäller alla behandlingar inom HR-området är av detta slag och här finns det stora osäkerhet hur status är när det gäller såväl informationssäkerhet som skydd för personuppgifter.

5.4.3 Råd och rekommendation

Det är väsentligt för kontoret att ha ordning på alla personuppgiftbehandlingar ur ett dataskyddsperspektiv varför det är nödvändigt att ha en organisation som kan få fram ovan angivna underlag för att kunna riskbedöma de behandlingar som sker i centrala IT-system.

Informationsägaren bör via fastighetsdirektören eller ansvarig för dataskydd följa upp frågan och ställa krav på att samtliga underlag av denna typ av IT-tjänst är samlad och tillgängliga för berörda informationsägare om ansvaret ska ligga lokalt hos kontoret.

5.5 Information om och kontaktuppgifter till DSO

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
x	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

Varje nämnd i Stockholms stad har utnämnt ett DSO som anmälts till Integritetsskyddsmyndigheten (”IMY”). Genom att utse och anmäla in ett DSO till IMY gäller GDPR:s regler i förhållandet mellan nämnden och DSO (GDPR art. 37-39 samt Riktlinje om dataskyddsombud (WP 243/2016)).

5.5.1 Krav enligt GDPR

Av GDPR (art. 38.4-5) framgår det att den registrerade får kontakta DSO med avseende på alla frågor som rör behandlingen av dennes personuppgifter och utövandet av dennes rättigheter enligt GDPR. DSO ska när det gäller genomförande av sina uppgifter vara bundet av sekretess bland annat i enlighet med svensk rätt. I dataskyddslagen (SFS 2018:218, 8 §) anges att DSO inte obehörigen får röja det som han eller hon vid fullgörandet av sin uppgift har fått kännedom om. Denna tystnadsplikt förutsätter att en registrerad ska kunna komma i kontakt med DSO och lämna information utan att DSO får föra informationen vidare annat än om den registrerade givit sitt samtycke. Då det kan röra sig om en registrerad som är anställd är tystnadsplikten viktig att upprätthålla för att skydda den anställde.

GDPR ställer även krav på att DSOs kontaktuppgifter ska offentliggöras.

5.5.2 Observation

Det finns en sida på Stadens hemsida som heter Dataskyddsombud där det lämnas information om vem som är DSO i enskilda förvaltningar och kontaktuppgifter till DSO.

Denna sida innehåller för kontorets del ingen information om vem som är DSO. Inte heller på annan plats framgår det vem som är kontorets DSO. Dessutom anges en funktionsbrevlåda för GDPR som kontaktuppgift till DSO. Denna funktionsbrevlåda är inte någon exklusivt kontaktväg till DSO.

5.5.3 Råd och rekommendationer

Det ska vara möjligt att kontakta DSO utan att någon annan får veta att den registrerade kontaktat DSO. Det bör lämpligen finnas två kontaktuppgifter på den aktuella sidan dels en e-post där registrerad kan begära att få registerutdrag och liknande begäran dels en e-post där en registrerad kan komma i direktkontakt med DSO.

6. Planerade/Föreslagna granskningsområden under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Uppföljning av organisationen för det strukturella dataskyddsarbetet
- Uppföljning av informationen om personuppgifterna externt och internt särskilt kamerabevakning.
- Genomgång av utbildningsmaterial som finns för att rekommendera utbildningsåtgärder för att växla upp dataskyddsarbetet.
- Utvärdera registerutdragsprocessen.

6.2 Planerade granskningar

Då jag kommer att fortsätta som dataskyddsombud inom kontoret till och med första kvartalet 2025 kommer ytterligare observationer att lämnas löpande till ledningen och överlämnas till tillträdande DSO.

7. Övrigt att rapportera

7.1 Sammanfattning

Det är viktigt att den obligatoriska dataskyddsutbildningen som finns genomgås årligen av alla medarbetare och konsulter.

7.2 Syfte

För att skapa en bra dataskyddskultur inom en förvaltning är utbildning och information om dataskyddsregelverket viktigt att presentera på ett verksamhetsnära sätt.

7.3 Observation

Den inom Staden framtagna utbildningen ”Dataskydd i kommunal verksamhet, Grundkurs 2022) är väl genomförd i de delar av dataskyddsarbetet som den omfattar med ett undantag som rör DSO:s ansvar. Det är den operativa dataskyddsorganisationen och inte DSO som ska säkerställa att verksamheten följer GDPR.
Utbildningen innehåller i huvudsak:

- Grunder och definitioner
- Grundläggande dataskyddsprinciper
- Rättslig grund
- Registrerades rättigheter
- Allmän handling – GDPR
- Fritext och e-post
- Personuppgiftsincidenter

Utbildningen ska genomföras årligen. I början av december hade ca 40 % av medarbetarna (73/187) på kontoret genomfört utbildningen.

7.4 Råd och rekommendationer

Det är viktigt att den obligatoriska dataskyddsutbildningen genomgås årligen av alla medarbetare och konsulter då den är bra i de delar av dataskyddsarbetet som den tar upp. Ytterligare utbildningsinsatser behöver dock övervägas för de funktioner som har ansvar för andra delar av dataskyddsarbetet. Det finns flera framtagna utbildningar inom Staden som kan vara lämpliga att genomgå för utvalda grupper av organisationen. Även riktad information om skyldigheter enligt GDPR kan tas fram av mig som DSO.

8. Ansvar enligt GDPR

8.1 Ansvar och roller inom Staden

Avsikten med detta avsnitt är att försöka få bättre klarhet över de regelverk som styr ansvar och roller kring informationssäkerhet och dataskydd inom Staden som helhet. Det finns vissa styrande dokument som anger huvudriktningen för ansvar och roller som även gäller för alla nämnder och styrelser. Denna kartläggning har varit avgörande för att kunna förstå det lokala dataskyddsarbetet och hur ansvaret är fördelat inom Staden.

8.1.1 Överordnade beslut om informationssäkerhet

Kommunfullmäktige har beslutat genom ”Reglemente med allmänna bestämmelser för Stockholm stads nämnder”, 2023:09, 5§, följande:

”Nämnden är personuppgiftsansvarig för de personuppgifter som nämnden behandlar i sin verksamhet. Nämnden kan också vara personuppgiftsbiträde åt en annan nämnd eller gemensamt personuppgiftsansvarig tillsammans med en annan nämnd, varvid de inbördes ansvarsförhållandena ska regleras. Vid ett biträdesförhållande ska den personuppgiftsansvariga nämnden ge instruktioner om behandlingen till den personuppgiftsbiträdande nämnden. Om gemensamt personuppgiftsansvar förekommer ska fördelningen av ansvar regleras mellan nämnderna, bl.a. avseende den registrerades rättigheter och tillhandahållande av information till den registrerade.”

I Riktlinje för informationssäkerhet i Stockholms stad (2022-02-21) som gäller i samtliga nämnder och styrelser står bland annat följande:

Stadens kvalitetsarbete … ställer krav på att staden utför ett grundläggande och systematiskt informationssäkerhetsarbete i alla sina verksamheter. Denna riktlinje anger kommunfullmäktiges direktiv för detta arbete. Arbetet ska i sin tur bidra till att staden upprätthåller trygghet och förtroende hos medborgare, näringsliv och besökare, men också att lagar, förordningar och riktlinjer efterlevs. Dagens informationssamhälle har lett till att grundläggande samhällsfunktioner är beroende av information i digitala tjänster. Detta beroende innebär i sin tur risker. Därför har kraven på skydd för information skärpts avsevärt genom lagstiftning, exempelvis dataskyddförordningen och NIS-direktivet samt regeringens strategi på nationell nivå. Både stadens ambitioner och svensk lagstiftning förutsätter en ändamålsenlig informationssäkerhet i stadens nämnder och styrelser…

… Dataskydd innebär skydd av personuppgifter enligt kraven i dataskyddsförordningen. Dataskydd är en del av informationssäkerhetsarbetet i staden…

8.1.2 Nämnders övergripande ansvar

I tillämpningsanvisning till stadens riktlinjer för informationssäkerhet (2024-11-13) är nämnder informationsägare och personuppgiftsansvariga för sin verksamhets personuppgiftsbehandling (1.4.2).

Nämnderna ansvarar för att det finns ett ändamålsenligt och effektivt informationssäkerhetsarbete inom den egna verksamheten samt att stadsövergripande riktlinjer och lagkrav efterlevs.

Nämnderna är dessutom i egenskap av personuppgiftsansvariga enligt dataskyddslagstiftningen skyldiga att instruera medarbetare m.fl. om hur personuppgifter får behandlas, genom rutiner och instruktioner.

Informationsägare ska fatta beslut om informationens skyddsvärde samt ställa krav på skyddsåtgärder och är ansvarig för att adressera skyddsåtgärder till rätt part. Informationsägaren ska omvärdera skyddsvärdet vid ändrade förhållanden på årlig basis.

En personuppgiftsansvarig är den som bestämmer ändamål och medel för en personuppgiftsbehandling. Om en nämnd utför behandlingen åt en annan nämnd uppstår ett internt personuppgiftsbiträdesförhållande som dock inte kan regleras genom avtal då Staden är en juridisk person. Inom staden ska det bestämmas vilken nämnd som är ansvarig och vilken som är biträden innan en behandling sker. Rollerna, ansvarig, gemensamt ansvarig och biträde behöver bestämmas och regleras så att alla parter vet vem som ska göra vad. Det är även viktigt att tydligt dokumentera dessa förhållanden på en gemensam yta. Vid interna arrangemang där flera nämnder är inblandade så är det viktigt att även informera de registrerade om arrangemanget och hur man kan ta tillvara sina friheter och rättigheter.

8.1.3 Förvaltningschefens ansvar

Förvaltningschef är nämndens operativa informationsägarrepresentant i verksamheten och ansvarar bland annat för att organisera verksamheten så att informationsägaransvaret och personuppgiftsansvaret kan omhändertas i linjen (1.4.2).

Förvaltningschef ska utse en informationssäkerhetssamordnare (nedan ISAM) som leder och samordnar det operativa arbetet med informationssäkerhet inom nämnden.

En Lokal anvisning för informationssäkerhet (1.4.2) ska fastställas av förvaltningschef med beskrivning av hur stadens övergripande ledningssystem för informationssäkerhet omsätts i den egna verksamheten. Den lokala anvisningen ska ses över årligen. Anvisningen ska beskriva ansvarsfördelning och roller inom egen informationssäkerhetsorganisation samt om specifik lagstiftning ska beaktas i verksamheten.

Förvaltningschef beslutar om nödvändiga resurser, mandat och befogenheter för de funktioner som arbetar med informationssäkerhet

8.1.4 Uppföljning av informationssäkerhetsarbetet

Den årliga rapporten Ledningens genomgång ska sammanställas av ISAM och lämnas till förvaltningschefen och omfatta en genomlysning av informationssäkerhetsarbete och ge underlag för förbättringar inför kommande verksamhetsår. Rapporteringen ska även innefatta dataskydd utifrån vad som framkommer i DSOs GDPR-årsrapport. Förvaltningschefen beslutar aktiviteter inom de två områdena för att uppnå tillräcklig kontroll.

8.1.5 Objektägare och objektstyrgrupp

Objektägare ansvarar för informationssäkerhetsarbetet i en IT-tjänster utöver ansvar för drift underhåll och utveckling av IT-tjänsten (Tillämpningsanvisning till stadens riktlinje för informationssäkerhet, 1.4.2). Vem som ansvara för dataskyddsfrågorna som rör IT-tjänster är inte lika tydligt uttalat. Det får antas att det ändå är objektägaren som ansvarar för dataskyddsfrågorna.

Det finns en objektsägare för alla IT-tjänster som hanterar personuppgifter inom Stadens verksamheter. Det gäller även om IT-tjänsten levereras av en extern system- eller tjänsteleverantör Objektägaren rapporterar till en Objektstyrgrupp som ansvarar för att leda informationssäkerhetsarbetet. Även här är det oklart vem av dessa som ansvarar för att dataskyddsarbetet följer GDPR.

8.1.6 Chefer inom verksamheten

Ansvaret för att skydda information i staden är decentraliserat och innebär att chefer som närmast ansvarar för en verksamhet har del i detta ansvar.

Chefen ansvarar för att den egna verksamhetens informationshantering följer riktlinjer för informationssäkerhet. Därför ska varje chef tillse att det kartläggs vilken typ av information som just deras verksamhet hanterar samt att den mest

betydelsefulla informationen, inte minst känsliga och integritetskänsliga personuppgiftsbehandlingar, är klassade.

Chefen ska tillse att de skyddsåtgärder som följer av klassningen på ett pragmatiskt sätt arbetas in i verksamhetens ordinarie linjearbete. Det ska vara tydligt vem i chefens linjeverksamhet som ansvarar för vilken åtgärd. Med skyddsåtgärder avses exempelvis att en uppföljning av behörigheter sker regelbundet, att en riktlinje eller anvisning tas fram, att personalen är informerad om sitt ansvar för informationssäkerhet med mera.

8.2 Närmare om GDPRs krav på personuppgiftsansvarig och biträde

Det avsnitt som återges nedan har flyttats ut ur Stadens obligatoriska styrdokument ”Tillämpningsanvisningar till stadens riktlinje för informationssäkerhet” vid den senaste revideringen som beslutades av stadsdirektören 2024-11-13. Ändringen beskrivs enligt följande: ”Minskad omfattning genom att vägledande (ej styrande) textstycken har flyttats ut.” I Nyhetsbrev till ISAM uppger Funktionen för stadsövergripande informationssäkerhet att ”uppdateringarna förändrar inte innehållet i sak, utan syftar till att förstärka och förtydliga de anvisningar som redan är beslutade”.

Då avsnittet är det enda som visar på ansvarsskyldigheten enligt GDPR för personuppgiftsansvarig samt för biträden har jag valt att återge avsnittet här.

”Nedan följer en exemplifierande beskrivning av det ansvar och skyldigheter som följer av rollerna personuppgiftsansvarig respektive personuppgiftsbiträde inom staden.

Den personuppgiftsansvariges ansvar

Den personuppgiftsansvarige nämnden eller styrelsen behöver bland annat säkerställa följande.

- Personuppgiftsbehandlingen ska ha en laglig/rättslig grund. Den ska fastställas för alla befintliga behandlingar och innan en ny behandling påbörjas.
- De grundläggande principerna (artikel 5 i dataskyddsförordningen) ska implementeras i själva personuppgiftsbehandlingen av verksamheten, dvs. i verksamhetens processer.
- Om känsliga personuppgifter behandlas ska ett lagstadgat undantag från det generella förbudet för behandlingen

kunna tillämpas. Om uppgift om brott behandlas ska gällande lagstiftning iakttas.
- Den registrerade, personen vars personuppgifter behandlas, har rätt till information om den specifika behandlingen och registrerades övriga rättigheter ska beaktas.
- Inbyggt dataskydd och dataskydd som standard ska tillämpas.
- Endast anlita personuppgiftsbiträden som kan garantera att registrerades rättigheter skyddas, att tekniska och organisatoriska åtgärder som är förenliga med gällande lagstiftning implementeras, samt att personuppgiftsbiträdesavtal med instruktion, alternativt stadenintern instruktion för personuppgiftsbehandling, tecknas.
- Register över personuppgiftsbehandlingarna, registerförteckning, ska upprättas.
- Tekniska och organisatoriska skyddsåtgärder ska implementeras, upprätthålls och utvärderas enligt gällande dataskyddslagstiftning och dataskyddspraxis, ex. artikel 32 i dataskyddsförordningen.
- Personuppgiftsincidenter ska kunna upptäckas och anmälningspliktiga personuppgiftsincidenter ska anmälas till tillsynsmyndigheten. Informationsskyldigheten gentemot den registrerade om en personuppgiftsincident ska uppfyllas.
- Konsekvensbedömning avseende dataskydd ska genomföras när så erfordras.
- Dataskyddsombud ska utnämnas.
- Tredjelandsöverföring av personuppgifter ska följa dataskyddslagstiftningens krav.

Personuppgiftsbiträdets ansvar

Personuppgiftsbiträdande nämnd eller styrelse behöver bland annat säkerställa följande.
- Register över personuppgiftsbehandlingar, registerförteckning, som utförs för den personuppgiftsansvariges räkning ska upprättas.
- Medverka och säkerställa att personuppgiftsbiträdesavtal med instruktion, alternativt stadenintern instruktion för personuppgiftsbehandling, tecknas.
- Bistå personuppgiftsansvarig med anledning av begäran om utövande av den registrerades rättigheter.
- Upprätthålla och utvärdera säkerheten för personuppgiftsbehandlingen och vidta de tekniska och organisatoriska åtgärder som krävs enligt gällande dataskyddspraxis.

- Underrättelseskyldigheten gentemot den personuppgiftsansvarige, dvs. att utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident lämna lagstadgad information.
- Bistå personuppgiftsansvarig, så denne kan lämna lagstadgad information till den registrerade vid en personuppgiftsincident.
- Vid behov och begäran av personuppgiftsansvarig bistå vid utförande av konsekvensbedömning avseende dataskydd.
- Utnämna dataskyddsombud.
- Vidta åtgärder för att säkerställa laglig tredjelandsöverföring.”

Utöver dessa grundläggande krav enligt GDPR finns ytterligare skyldigheter för en personuppgiftsansvarig att följa, som bland annat det omfattande informationskravet mot registrerad för att en behandling får genomföras samt krav gällande DSOs arbetssituation och ställning.

Ansvarsskyldigheten gällande dataskydd ligger i väsentliga delar utanför traditionellt informationssäkerhetsarbete varför det är lämpligt att reglera dataskyddsarbetet särskilt inom en verksamhet.

Bilaga 1

Begäran om uppgifter inför GDPR- årsrapport 2024.

Följande områden är obligatoriska att redovisa i dataskyddsombudets GDPR - Årsrapport

Då rapporten ska lämnas till respektive förvaltning vid lucia i år är tiden knapp för mig att inhämta underlag till den obligatoriska delen. Jag ber er om möjligt prioritera dessa frågor. Jag vore tacksam för att få svar inom en vecka och senast den 3 december. (Det är bra om ni svarar i vart fall övergripande. Dataskyddsarbete är en löpande process där skyddet byggs på eftersom.

Jag är tacksam för att få svar på följande frågor:

1. Registerförteckning
Då jag har tillgång till registret eller i vart fall fått en kopia av det så vet jag omfattningen av registret.

Det finns många sätt att föra register på när det gäller behandling av personuppgifter.

- Ange gärna logiken för ert register. Det finns ingen logik för vår registerförteckning. Jag har en sammanfattning av arbetet med Draftit skriven år 2023 av tidigare DSO hos Combitech och tidigare dataskyddssamordnare, som du kan få som handlar om strukturen i den.

Register kan omfatta lagringsplatser och system, processer eller behandlingar och slutligen tjänsteleverantörer där behandlingar utförs.

- Vad omfattar ert register?
- processer
- system
- fysiska pärmar
- enstaka dokument
- advokatbyråer
- webbplatser
- applikationer och aktiviteter i olika processer

Vem gör vad?

- Vem ansvarar för registerförteckningen? Respektive informationsägare, ofta avdelningschefer.

- Finns det en lokal rutin kring registerföring (om Ja – var finns den)?

  Det finns en lathund som heter ”Lathund för att uppdatera behandlingar i Draftit Records för standardanvändare.” Men den visar enbart hur handläggare ska uppdatera sina egna behandlingar som de är ansvariga för i Draftit. Finns på samarbetsytan för GDPR: Verksamhetsledning och stöd - GDPR direkt på första sidan ligger den som ett separat Word dokument.

- Vem ansvarar för att processer/behandlingar registreras? Den som är produktadministratör, dataskyddssamordnare har det varit hittills som genomför det praktiska arbetet i Draftit.

- Revideras uppgifterna i registret löpande?(Om Ja ange intervall.) Nej, det har inte gjorts på flera år. Just nu håller Jenny på och uppdaterar kontaktuppgifter till ansvariga personer för behandlingarna. Det verkar inte finnas någon rutin när medarbetare slutar att de kollar upp vem som ska ersätta deras uppgifter i Drafit.

2. Styrdokument

När det gäller styrdokument som har påverkan på dataskyddsarbetet så kan jag se två områden där det kan finnas information om hur dataskyddsarbetet är organiserat, dels i ledningssystemet och i delegations-beslut dels som en del av informationssäkerhetsarbetet.

I många organisationer finns det en tydlig avsändare på de styrdokumenten som bereds och antas inom en organisation. Det brukar även finnas en reglering om när ett styrdokument ska uppdateras och att det anges i dokumentet när det är gjort och även vad som ändrats så att det står klart för de berörda inom organisationen. Jag har när det gäller dataskyddsfrågorna inte hittat någon tydlig linje i de styrdokument som jag hittat. Jag vill därför få svar på följande:

- Vilka lokala styrdokument har ni antagit som rör dataskyddsfrågor (Delegationsordning, Ledningens Genomgång, lokal anvisning om informationssäkerhet etc)? Delegationsordning, Ledningens genomgång, lokal anvisning om informationssäkerhet

- Är alla lokala styrdokument upplagda på nya intranätet? eller finns det styrdokument på andra platser? Nej fastighetskontoret har inga styrdokument kopplat till GDPR upplagda på Intranätet, alla styrdokument som finns är upplagda i Sharepoint på samarbetsytan: Verksamhetsledning och stöd - GDPR.

- Vem är ansvarig för de olika styrdokumenten?

  - Delegationsordning har juristerna ansvar för att ta fram.
  - Rapporten Ledningens genomgång Informationssäkerhet 2024 ansvarar enhetschef IT och Strategi för, och nästa år tar säkerhetschefen över ansvaret för denna.
  - Lokal anvisning om informationssäkerhet ansvarar säkerhetschefen för och IT och strategi ansvarar för ett antal bilagor till dokumentet

3. Organisatoriska och tekniska åtgärder - Informationsklassning

Denna punkt rymmer många åtgärder men det obligatoriska området avser endast frågan om behandlingarna har informationsklassats. Om jag inte minns fel fans det en inriktning att under 2024 göra i vart fall en inventering av behandlingarna med lite högre risk gällande informationsklassning.

Informationsklassningar

- Vem har ansvar för att det sker en informationsklassning? Enligt ”Handbok för informationsklassning” (se sid 5, finns på Intranätet se Informationsklassning, riskanalys och konsekvensbedömning) är det Informationsägaren som ansvarar för att initiera informationsklassningar. Vilket också eftersträvats av en konsult som arbetat med informationsklassning även om processen inte varit igång så länge.
- Har ni gått igenom alla behandlingar som har tagits upp i registret? Nej alla har inte gåtts igenom, det finns ett par som inte är klassade och det var länge sen som risknivån klassades på många av dem.

- Hur många personuppgiftsbehandlingar har informationsklassats totalt och under året? 0 under detta

år, av totalt 67 behandlingar är det 4 st som inte har klassats alls.

- Finns det en plan för att löpande riskbedöma behandlingarna? Om ja vad innebär den i korthet. Nej det finns ingen plan för det.

4. Konsekvensbedömningar

Att känna till vilka behandlingar som sker eller som planeras inom en verksamhet är en viktig grundförutsättning för ett systematiskt dataskyddsarbete. En konsekvensbedömning är avsedd att lyfta fram behandlingar med högre risker i ett tidigt skede så att det finns möjlighet att ställa krav (på uppgiftsminimering, skydd, och andra åtgärder) såväl vid utveckling som inför upphandling av en tjänst eller vid en ändrad användning. Den så kallade tröskelanalysen utgår från de riskkriterier som framgår av dataskyddsförordningen samt av de riktlinjer som tillsynsmyndigheten IMY tagit fram.

- Har ni identifierat alla behandlingar med hög risk? Har ni genomfört en tröskelanalys för att se om det är nödvändigt med en konsekvensbedömning? Nej inga identifieringar av behandlingar med hög risk har genomförts år 2024.

- Har ni genomfört de konsekvensbedömningar som har identifierats? N/A

- Vem är ansvarig för att det sker en tröskelanalys eller konsekvensbedömning? Avdelningschef i samverkan med dataskyddsombud.

- Finns det en rutin för att uppdatera gjorda konsekvensbedömningar med viss regelbundenhet?

Det är denna rutin som finns avseende konsekvensbedömningar på GDPR samarbetsyta:
https://samarbete.stockholm.se/sites/FSKinternadokument/GDPR/4.%20Anvisningar%20och%20mallar/Riskanalys%20och%20konsekvensbed%C3%B6mning/Riskanalysmall%202019-03-22%20v1.1.docx?d=wd043d44b38dd41199fdb6fa8be86b998

Men jag tror senast konsekvensbedömningar gjordes i ett större skala var i samband med ”Riskanalys och konsekvensbedömning av personuppgiftsbehandlingar inom ramen för projekt ITFF” år 2019, diarienummer FSK 2019/629.

Material från arbetet finns också på gruppdisk: \\ad.stockholm.se\cli-sd\cc2sd007\006432\GDPR se även FSK Gemensamt\Riskananlyser_&_konsekvensbedömningar

5. Registrerades rättigheter

Denna punkt är viktig då bland annat tillsynsmyndigheten IMY har haft fokus på de registrerades rättigheter i sin tillsynsverksamhet. Det är viktigt att fånga upp begäran från registrerad i verksamheten.

- Hur många ”begäran från registrerad” (om exempelvis registerutdrag, rättelser, begränsningar m.m.) har kommit in hittills i år? 1 st.

- Hur stor andel av dessa har hanterats inom 30 dagar? Samtliga.

- Vem sköter det praktiska arbetet med begäran? Dataskyddssamordnaren samordnar detta i samarbete med berörda systemägare i verksamheten med kunskap om olika system.

- Finns det en rutin för detta arbete? Ja det finns en rutin på GDPR:s samarbetsyta: https://samarbete.stockholm.se/sites/FSKinternadokument/GDPR/4.%20Anvisningar%20och%20mallar/Registerutdrag. Då dessa rutiner är några år gamla och är i behov av uppdatering så gjorde vi i år en logg på de steg vi följde och förslag på utveckling av rutinen, den finns också på GDPR samarbetsyta: https://samarbete.stockholm.se/sites/FSKinternadokument/GDPR/4.%20Anvisningar%20och%20mallar/Registerutdrag, och är diarieförd i FSK 2024/510.

6. Personuppgiftsincidenter

Jag är medveten om att det finns ett system för att anmäla in incidenter - IA. Precis som alla system så finns det vissa brister som påverkar hantering av personuppgiftsincidenter. Vid förlust av en PC eller telefon så kan den incidenten även omfatta en personuppgiftsincident. Då det endast går att styra incidenten till en kategori inom IA kan det vara så att alla personuppgiftsincidenter inte kommer att anmälas som de ska.

- Vem har ansvaret för att anmäla en personuppgiftsincident till tillsynsmyndigheten? Enligt 3. Rutin personuppgiftsincidenthantering 2019-01-07 v1.3.docx är avdelningscheferna ansvariga för detta i samarbete med dataskyddsombud.

- Hur många incidenter har inträffat hittills i år? Inga som vi fått vetskap om.

- Hur många incidenter har anmälts inom normal tid (72 timmar) från det att de var konstaterade av personuppgiftsansvarig? -

- Finns det någon rutin för hur incidentrapporteringen ska gå till och vem som ansvarar för vad? Var finns den i så fall? Den finns på GDPR:s samarbetsyta: 3. Rutin personuppgiftsincidenthantering 2019-01-07 v1.3.docx. Det står vem som ansvarar för vad i denna, även om den är daterad och från år 2019. Det som gällde då var att medarbetaren som var arkivarie även var dataskyddsombud.

- Följer ni upp hur incidenterna anmäls i systemet för att kunna fånga upp personuppgiftsincidenter som anmälts in som någon annan typ av incident?

Inte vad dataskyddssamordnare eller Olga Ekstam, avdelningschef verksamhetsstöd, känner till.