STOCKHOLMS STADSHUS AB
En del av Stockholms stad

2023-01-31

Utfallsrapport VB 2022
S:t Erik Försäkrings AB

Stockholms Stadshus AB	Org.nr 556415-1727			
Postadress	Besöksadress	Telefon	Fax	E-post
105 35 STOCKHOLM	Stadshuset, 3 tr.	08-508 290 00	08-509 290 80	info@stadshusab.se

Innehållsförteckning

Bilagor

Bilaga 1: Årsrapport GDPR 2022 och plan 2023 SEF

Bilaga 2: Utfall 22-12

Sammanfattande kommentar

Årets resultat uppgår till 17 mnkr före bokslutsdispositioner och skatt jfr med budgeterat 1 mnkr. Resultatet beror till stor del på att skadekostnaderna varit lägre än budgeterat. Samtidigt har kostnaderna för återförsäkring ökat beroende på bolagets historiska skaderesultat.

Solvenskapitalkvoten (SCR-kvoten) per den 31 december har ökat till följd av ett bra skadeår med positivt resultat och uppgår till 384 % (VB 2021: 296 %).

Det skadeförebyggande arbetet har utökats genom samarbete med KTH samt arbete med stadens brandskyddsnätverk.

Analys av ekonomisk utveckling

Årets resultat uppgår till 17 mnkr före bokslutsdispositioner och skatt. Det som har haft stor påverkan på resultatet och avviker från de senaste åren är lägre skadekostnader. Där utöver har administrationskostnaderna kunnat hållas på i stort sett oförändrad nivå. Trots att återförsäkringskostnaderna har ökat pga historiska skadekostnader innebär bolagets verksamhet under 2022 ett resultat över budget.

Solvenskapitalkvoten (SCR-kvoten) per den 31 december är 384% (296). Det är god marginal till styrelsens limit på minst 150 procent och lagkravet om minst 100 procent.

Bedömning av bolagets interna kontroll

Bolaget bedömer att den interna kontrollen under år 2022 varit tillräcklig.

Som försäkringsbolag har bolaget ett lagstadgat krav på ett flertal centrala funktioner som utför granskningar utöver verksamhetens egna och revisorerna. Dessa funktioner är aktuariefunktion (försäkringsmatematiska granskningar), regelefterlevnadsfunktion (legal kontroll), riskhanteringsfunktion (bolagets samlade risker) samt internrevision (granskar de centrala funktionerna samt bolagets interna kontroll och styrning). Funktionerna rapporterar till styrelsen och verksamheten. Utöver detta sker verksamhetens egna granskningar i första linjen.

Verksamhetens egna granskningar har skett enligt plan. Samtliga centrala granskningsfunktioner har genomfört sina granskningar och internrevision i sin tur granskat funktionerna och den övergripande interna kontrollen och styrningen av företaget. Rapportering har skett till styrelse och verksamhet.

1. En modern storstad med möjligheter och valfrihet för alla

S:t Erik Försäkring medverkar utifrån sina förutsättningar till Stockholms stads insatser för att få fler stockholmare i arbete.

Med anledning av de legala krav på kompetens och utbildning som finns för att arbeta i ett livförsäkringsbolag har S:t Erik Försäkring små möjligheter att själv erbjuda arbetssökande kvalificerad yrkeslivserfarenhet genom praktikplatser.

Bolaget tillhandahåller istället försäkringslösningar som underlättar för stadens enheter i deras arbete inom området.

1.1 I Stockholm är människor självförsörjande och vägen till arbete och svenskkunskaper är kort

Bolaget har på grund av sin storlek och sin högt specialiserade verksamhet inte någon möjlighet att erbjuda varken platser för kommunal visstidsanställning eller feriejobb under verksamhetsåret. (Finansinspektionen ställer höga krav på kompetens för att få arbete i försäkringsbolag).

Bolaget tillhandahåller försäkringslösningar för att underlätta för andra av stadens enheter att ex ta emot praktikanter.

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
	Antal aspiranter som fått Stockholmsjobb ***Analys*** Bolaget tillhandahåller försäkringslösningar för att bistå andra enheter i deras uppfyllande av indikatorn.	0 st	0 st	
	Antal tillhandahållna platser för feriejobb ***Analys*** Bolaget tillhandahåller försäkringslösningar för att bistå andra enheter i deras uppfyllande av indikatorn.	0	0 st	
	Antal tillhandahållna platser för kommunala visstidsanställningar ***Analys*** Bolaget tillhandahåller försäkringslösningar för att bistå andra enheter i deras uppfyllande av indikatorn.	0	0 st	
	Antal tillhandahållna platser för Stockholmsjobb ***Analys*** Bolaget tillhandahåller försäkringslösningar för att bistå andra enheter i deras uppfyllande av indikatorn.	0	0 st	
	Antal ungdomar som fått feriejobb i stadens regi ***Analys*** Bolaget tillhandahåller försäkringslösningar för att bistå andra enheter i deras uppfyllande av indikatorn.	0 st	0 st	

1.2. Stockholm är en trygg, säker och välskött stad att bo och vistas i

S:t Erik Försäkring arbetar för att staden har ett risk- och säkerhetsmedvetande så att skador förebyggs, att stadens tjänster alltid fungerar och att stadens försäkringskostnader minimeras, bland annat genom att ge stöd till stadens nämnder och bolagsstyrelser i arbetet med att identifiera risker samt att förebygga och minimera skadeverkan. S:t Erik Försäkring förvaltar stadens incidentrapporteringssystem (IA). Staden har en etablerad samverkan med S:t Erik Försäkring i det olycksförebyggande arbetet på både central och lokal nivå.

Bolaget genomför regelbundet kartläggning över affärsprocesser och affärsverksamheter, affärsfunktioner, roller och tillgångar (t.ex. informationstillgångar och IKT-tillgångar).

Vidare har bolaget haft kontinuerlig dialog med stadens förvaltningar och bolag gällande det dagliga risk- och säkerhetsarbetet, utbildning och rådgivning i handhavande av stadens incidenthanteringssystem IA, riskbesiktning av ett antal av stadens byggnader och verksamheter med efterföljande skadeförebyggande rekommendationer, regelbunden rådgivning och uppföljning av stadens SBA -arbete.

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
Stödja det olycks- och skadeförebyggande arbetet i kommunkoncernen med fokus på försäkringsbara risker samt risker som omfattas av lagen om skydd mot olyckor	Antalet genomförda riskbesiktningar ***Analys*** En besiktning omfattar ofta både byggnad samt verksamhet och resulterar således i 2 st rapporter. Båda dessa typer av rapporter benämns riskbesiktningar.	134	80	Projekt avseende brand i fastigheter med påbyggnader på taket. ***Analys*** Kommer att överföras att ingå i det strategiska arbetet under 2023.
	Antalet incidenter som rapporteras i stadens incidentrapporteringssystem . ***Analys*** En ökning från förra årets 18 244.	19 100	18 000	
				Nämnder och bolagsstyrelser ska omsätta lärdomar från krishanteringen av pandemin i uppdaterad beredskapsplanering, såsom krisledningsplanering, kontinuitetsplanering och krisledningsövningar ***Analys*** Bolagets krisplaner omfattar pandemi scenarie.
				Översyn informationsklassningar ***Analys*** IT-ansvarig har anställts och infoklassning påbörjats med konsult genom FKU av stadens konsulter.

1.3. I Stockholm når barn sin fulla potential då Stockholms skolor och förskolor är de bästa i Sverige

Inte relevant för bolaget.

1.4. I Stockholm får människor i behov av stöd insatser i tid präglade av hög kvalitet, evidens och rättssäkerhet

Inte relevant för bolaget.

1.5. I Stockholm har äldre en tillvaro som präglas av hög kvalitet, trygghet och självbestämmande

Inte relevant för bolaget.

2. En hållbart växande och dynamisk storstad med hög tillväxt

Genom att bolaget S:t Erik Försäkrings AB stödjer det olycks- och skadeförebyggande arbetet i kommunkoncernen med fokus på försäkringsbara risker samt risker som omfattas av lagen om skydd mot olyckor bidrar bolaget till en hållbart växande och dynamisk storstad med hög tillväxt.

2.1. Stockholm har Sveriges bästa företagsklimat och ett internationellt konkurrenskraftigt näringsliv

Bolaget bidrar till målet genom tillhandahållande av försäkringslösningar som ger stadens bolag och förvaltningar bättre förutsättningar att nå målet.

2.2. Stockholm byggs attraktivt, tätt och funktionsblandat utifrån människors och verksamheters skiftande behov

Inte relevant för bolaget.

2.3. Stockholms infrastruktur främjar effektiva och hållbara transporter samt god framkomlighet

Inte relevant för bolaget.

2.4. Stockholm är en modern kultur- och evenemangsstad med en stark besöksnäring

Inte relevant för bolaget.

2.5. Stockholm är en hållbar stad med en god livsmiljö

Bolaget bidrar i möjligaste mån till stadens miljöprograms genomförande. Genom att stödja bolagens förebyggande arbete kan klimatrelaterade skador minskas och därmed reduceras de försäkringsbara riskerna.

Verksamheten i bolaget ska ha en så låg negativ miljöpåverkan som möjligt.

Bolaget hyr av FSK och samverkar i den mån det är möjligt att minimera uppvärmning och minimerar elförbrukning genom att inte tillåta egna värmeelement samt införa process att siste person som lämnar kontoret tillser att allt som kan släckas är släckt.

Genom premiesättning och nivå på självrisk har bolaget strävat till att stadens egendomsförvaltande verksamheter har arbetat skadeförebyggande och därmed kunnat bidra till en hållbar stad och god livsmiljö.

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
				✔ Genom premiesättning säkerställa att

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
				klimatriskförebyggande arbete som även minskar försäkringsbara risker premieras. ***Analys*** Premiemodellen tar hänsyn till målet.

3. En ekonomiskt hållbar och innovativ storstad för framtiden

S:t Erik Försäkring har arbetat med att effektivisera sin administrativa processer för att begränsa stadens kostnader långsiktigt. Bolaget har också arbetat med att automatisera sina processer med hjälp av systemstöd, t.ex. ett projekt för elektroniska skadeanmälan. Samverkan med KTH har också etableras under året för att ta till vara forskningen i, och utveckla, det förebyggande arbetet.

3.1. Stockholm har en budget i balans och långsiktigt hållbara finanser

S:t Erik Försäkring försäkrar Stockholms stads samtliga verksamheter. Bolagets ekonomiska resultat påverkas till största delen av dess skaderesultat. Det övergripande långsiktiga ekonomiska målet är ett resultat efter finansnetto om 1 miljon kronor. Eftersom skadorna som försäkringsbolaget ska täcka varierar över tiden gör det att bolagets ekonomiska resultat också varierar.

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
	Andel administrations- och indirekta kostnader ***Analys*** Andelen administrations- och indirekta kostnader som indikator är mindre lämplig att använda för att mäta effektiviteten i ett sakförsäkringsbolag då bolagets administrativa kostnader ställs i relation till bolagets övriga kostnader som bland annat inkluderar samtliga skadekostnader. Då skadekostnaderna blir mindre än budgeterat ökar således indikatorn trots att administrationskostnaderna inte ökat. **Räknas alla bolagets kostnader är index 17,1%**	29,9 %	24 %	
	Avvikelse investeringsbudget, % ***Analys*** Bolaget saknar	0 %	0 mnkr	

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
	investeringsbudget.			
	Resultat efter finansnetto(mnkr) ***Analys*** Ett bättre skaderesultat innebär att vinsten överstiger den budgeterade om 1 mnkr.	17	1	
	SCR-kvot ***Analys*** Ett positivt resultat innebär att bolagets tillgångar ökar och SCR-kvoten ökar.	3,8	1,5	

3.2. Stockholm använder skattemedlen effektivt till största nytta för stockholmarna

S:t Erik Försäkring arbeta fortsatt med att effektivisera sin verksamhet.

Arbetet i företaget ska bedrivas så kostnadseffektivt som möjligt inom ramen för vad bolagets övriga mål tillåter. Bolagets rutiner ska kontinuerligt ses över för att om möjligt hitta nya metoder och hjälpmedel som kan öka effektiviteten och hålla de administrativa kostnaderna låga. En ökad grad digitalisering är en nödvändig väg.

S:t Erik Försäkring AB arbetar även för att staden har ett risk- och säkerhetsmedvetande så att skador förebyggs genom att ge stöd till stadens nämnder och bolagsstyrelser i arbetet med att identifiera risker samt att förebygga och minimera skadeverkan.

Bl.a. leder staden ett brandskyddsnät där en löpande dialog förs mellan S:t Erik Försäkring och stadens förvaltningar/bolaget kring risk- och säkerhetsfrågor så att olyckor och skador förebyggs.

Syftet med nätverket är att byta erfarenheter, höja kompetensen, bevaka omvärlden och få tillgång till forskningsrön inom området. KTH deltar löpande i nätverket.

S:t Erik Försäkring AB förvaltar stadens incidentrapporteringssystem (IA) som ska användas för inrapportering av incidenter.

För att säkerställa behovet av kompetenta och nöjda medarbetare arbetar bolaget kontinuerligt för att utvecklas som attraktiv arbetsgivare genom en tillitsbaserad styrning, kontinuerlig kompetensutveckling, flexibilitet avseende arbetsplats samt en positiv syn på friskvård under arbetstid.

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
Analysera och följa upp kommunkoncernens riskhanteringsarbete				
Effektivitetsmål	Driftskostnader i förhållande till premier för egen räkning ***Analys*** Driftskostnader ligger under budget genom att bolaget delar lokaler och viss personal med andra bolag.	24,6 %	26 %	
Genom premiesättning säkerställa att skademinimerande och				Anpassa priset på försäkringsskydden ***Analys***

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
riskförebyggande arbete premieras				Premiemodellen tar hänsyn till skador, skadeförebyggande arbete samt trender avseende skador och kostnader.
Kvalitetsmål för verksamheten				
Medverka och teckna samtliga sakförsäkringar som stadens nämnder och bolagsstyrelser har behov av	Andelen av koncernens försäkringar i procent som försäkras eller förmedlas av bolaget ***Analys*** Enligt plan.	100	100 %	
	Samtliga försäkringstagare ska erbjudas ett årligt förnyelsebesök. ***Analys*** Enligt plan.	100	100 %	
Optimera den försäkringsrisk som bolaget själv tar i förhållande till fastslagen risknivå				Vid upphandling av återförsäkring, optimera självbehållsnivåerna i förhållande till riskaptit och kostnaden för försäkringsskyddet ***Analys*** Fku har genomförts efter bedömning av möjligheterna att ändra självbehåll. Dessa kvarstår oförändarade.
	Aktivt Medskapandeindex ***Analys***	87	85	
	Andel upphandlade avtal där kontinuerlig uppföljning genomförts ***Analys*** Enligt plan.	100 %	100 %	
	Andel upphandlingar där marknadsdialog har genomförts ***Analys*** Enligt plan.	100 %	100 %	
	Index Bra arbetsgivare ***Analys***		84	

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
	S:t Erik Försäkrings AB har 2022 inget värde på index Bra arbetsgivare. Anledningen till detta är att bolaget inte har ett värde på delindex Jämställdhet.			
	Sjukfrånvaro ***Analys***	0,8 %	2,5 %	
	Sjukfrånvaro dag 1-14 ***Analys***	0,8 %	2,5 %	

Stockholms stad

GDPR Årsrapport

2022

S:t Erik Försäkrings AB

GDPR årsrapport
Januari 2023

Utgivningsdatum styrelsen: 2023-01-19
Kontaktperson: Erik Fischer

1 Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var 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. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnd och bolagsstyrelse behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett Dataskyddsombud (”DSO”). DSO:n har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för nämnd och styrelse att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnd eller bolagsstyrelse ska kunna *visa* att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna *dokumenteringsskyldighe*t. Årsrapporten är även ett medel för nämnds/bolagsstyrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

2 Sammanfattning

I egenskap av ert Dataskyddsombud ämnar jag följande årsrapport.

Bolaget har ett fåtal egna verksamhetssystem där personuppgifter behandlas, i övrigt används stadens IT-miljö.

Verksamheten är förvaltande, vilket innebär att behandlingar, personuppgifter och system sällan ändras.

Generellt har bolaget en god kontroll och struktur på hanteringen av personuppgifter. Det ringa antalet anställda (8 st ink. VD) innebär en mycket god direkt kunskap om system och personuppgifter samt innebär direkt tillgänglighet för spridning av personuppgifts-relaterad information.

Det finns ett behov av att genomföra informationsklassning på samtliga de behandlingar som genomförs och inte endast de i egna system. Vidare bör genomförda klassningar uppdateras årligen och dokumenteras.

Konsekvensbedömningar bör även de uppdateras årligen och dokumenteras.

Bolaget har anställt en IT-ansvarig som påbörjat klassningar, ett arbete som planeras fortsätta under 2023, och i samband med det planeras även uppdatering av konsekvensbedömningar.

3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som Personuppgiftsansvarig (”PUA”) som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som dataskyddsförordningen avser.

De obligatoriska rapporteringsområdena är registerförteckning, styrdokument, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter.

Nedan redogörs för nämndens eller bolagets status och DSO:ns slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	12
Har nödvändiga uppdateringar gjorts?	JA
Bedöms registerförteckningen vara fullständig?	JA
Har verksamheten lämpliga rutiner för registerföring?	JA

3.1.2 Syfte

För att något ska gå att skydda måste det först vara synligt för verksamheten. Det följer därför i klartext av dataskyddsförordningen (artikel 30) att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som behandlas i verksamheten, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde, och dokumentera dem i en så kallad registerförteckning (även kallat behandlingsregister).

3.1.3 Resultat

Verksamhetens samtliga behandlingar finns upptagna i registret som har uppdaterats under perioden. Registerförteckningen upptar alla de delar som ett register ska innehålla. Registerföringen har lämpliga rutiner för uppdatering.

3.1.4 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

3.1.5 DSO ger råd och rekommendationer till PUA

Inga rekommendationer.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	JA
Håller innehållet i de existerande dokumenten lämplig kvalitet?	JA
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	JA
Är dokumenten uppdaterade?	JA
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	JA

3.2.2 Syfte

Området syftar till att PUA genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar PUA till medarbetare i sin verksamhet om vad som gäller och vad som förväntas av medarbetarna, när de hanterar personuppgifter. Att styrdokument finns nedtecknade, beslutade och kommunicerade medför att medarbetaren får dataskyddsinformation och kan behålla kunskapen över tid och tillämpa den på ett konsekvent sätt. En röd tråd i Dataskyddsförordningen är att viktiga arbetssätt och rutiner ska vara dokumenterade.

3.2.3 Resultat

Verksamheten har styrdokument ”Riktlinje för hantering av personuppgifter”, senast uppdaterad 220523. Riktlinjen innehåller erforderliga rutiner och instruktioner för hantering av personuppgifter.

Vidare finns information till registrerade på hemsidan. Informationstexterna baseras på vilken roll registrerad har och omfattar de behandlingar som är aktuella.

3.2.4 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

3.2.5 DSO ger råd och rekommendationer till PUA

Inga rekommendationer.

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

3.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	Verksamheten har klassat eget verksamhetssystem samt IA-systemet. Information i stadens centrala system har inte klassats av verksamheten då verksamheten bedömt att detta sker centralt. Klassning av dessa kommer att ske under 2023.
Är klassade personuppgiftsbehandlingar aktuella?	NEJ – mer än 2 år sedan sist, inga förändringar har dock skett i behandlingar eller system, en pågående klassning. Infoklassning har påbörjats 2022 och fortsätter under 2023.

3.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd så ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Utan informationsklassningen har verksamheten inte förutsättningar att välja rätt åtgärder för att skydda sin information. Det är därför av stor betydelse för dataskyddsarbetet att PUA ges en uppdaterad bild varje år av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar.

3.3.3 Resultat

Verksamheten har klassat information avseende egna system (Insman) och ett stadsgemensamt (IA), men inte den information som finns i övriga stadsgemensamma system. Totalt har 2/12 behandlingar klassats.

Av verksamheten gjorda klassningar har en (Insman) inte uppdaterats och en (IA) uppdaterats, men behandlingarna eller systemen har inte ändrats sedan senaste klassning.

Stadens gemensamma system har en hög säkerhet, varför information som finns i dessa har låg risk.

3.3.4 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

Då behandlingar som ligger i stadens system inte klassats föreligger en brist mot stadens riktlinjer att all informationshantering ska klassas. Risken bedöms som låg då dessa system har hög säkerhet.

Klassningar som inte har uppdaterats - de personuppgifter som behandlas och systemens utformning avseende säkerhet är samma som sedan senaste klassningen, varför risken bedöms som låg.

Då IT-ansvarig anställts och infoklassningar påbörjats är den sammantagna risken låg.

3.3.5 DSO ger råd och rekommendationer till PUA

Verksamheten bör klassa samtlig informationshantering och uppdatera tidigare gjorda klassningar. För information i centrala system (stadens) kan ev. utförda centrala klassningar dokumenteras och justeras efter verksamhetens förutsättningar.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	JA
Har alla potentiella högriskbehandlingar konsekvensbedömts?	NEJ. Information i IA har klassats under 2022 och konsekvens-bedömning ska göras under 2023. Säkerheten i IA är så pass hög (används av flera kommuner avseende arbetsmiljö) att risken för konsekvenser är liten.
Är de genomförda bedömningarna aktuella?	NEJ, informationen och systemen har dock inte ändrats sedan tidigare konsekvensbedömning, Ny bedömning kommer att göras under 2023 allteftersom systemen klassas.

3.4.2 Syfte

Konsekvensbedömningen hjälper en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas i projekt eller linjeverksamhet. En konsekvensbedömning har till syfte att identifiera och dokumentera risker kopplade till en viss behandling, samt att bedöma sannolikheten och konsekvensen om riskscenariot skulle inträffa. Baserat på bedömningen kan/ska riskförebyggande åtgärder vidtas.

3.4.3 Resultat

4 behandlingar som bör konsekvensbedömas har identifierats:

a. Insman försäkrings/skadesystem
b. Belivia skadeanmälningsmodul
c. Hantering av information kring arbetstagare
d. IA (avseende arbetsskador)

Behandlingar a-c har utförts, men inte uppdaterats, d kvarstår att konsekvensbedömas efter genomförd klassning.

3.4.4 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

Behandlingen i IA - Systemet har hög säkerhet och används av flertalet kommuner (bla avseende arbetsskador). Risken bedöms som låg.

Ej uppdaterade konsekvensbedömningar - personuppgifterna och systemens säkerhet har inte ändrats. Risken bedöms som låg.

3.4.5 DSO ger råd och rekommendationer till PUA

Verksamheten bör göra en konsekvensbedömning av behandlingen i IA samt uppdatera de andra gjorda konsekvensbedömningarna.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	0
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	0

3.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen (artikel 12–22) ett antal rättigheter som på olika sätt ska garantera att den registrerade personen har insyn i hur dennes personuppgifter hanteras samt har en viss kontroll över personuppgiftsbehandlingen. Det är ett krav enligt förordningen att den verksamhet som enligt förordningen är att se som personuppgiftsansvarig – dvs. i stadens fall nämnder och bolag – tillgodoser rättigheterna i fråga.

Rättigheterna medför en rätt att ställa krav på att verksamheten vidtar vissa åtgärder, som exempelvis att lämna ut ett så kallat registerutdrag eller att rätta vissa uppgifter. (Radering, den så kallade ”rätten att bli glömd”, är sällan aktuell i någon större mån eftersom stadens verksamheter lyder under krav på bevarande till följd av offentlighetsprincipen.) Verksamheten har enligt dataskyddsförordningen artikel 12.3 en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran. (Notera dock att det finns undantagssituationer angivna i artikel 12.3, där fristen kan förlängas till mer än en månad.)

3.5.3 Resultat

Verksamheten har under perioden inte fått begäran om registerutdrag.

3.5.4 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

3.5.5 DSO ger råd och rekommendationer till PUA

Inga rekommendationer.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Löpande av verksamheten, inrapportering sker i IA samt eget register. 3 st för 2022.
Hur många personuppgiftsincidenter har dokumenterats?	3/3
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	0
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	N/A

3.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen (artikel 4.12) ”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.”

I en verksamhet kan förekomma många andra typer av incidenter, som inte involverar personuppgifter. Det är viktigt att hålla den saken i åtanke, så att årsrapporteringen inte omfattar annat än just personuppgiftsincidenter. Vidare är det en grundförutsättning för hanteringen av personuppgifter att incidenter över huvud taget upptäcks, samt att verksamheten förstår att hantera incidenter som rör personuppgifter på det särskilda sätt som dataskyddsförordningen kräver.

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland dataskyddsförordningens olika verktyg för att åstadkomma en sund personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering.

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringsskyldigheten gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (se artikel 33). Detta innebär att de flesta personuppgiftsincidenter ska rapporteras till IMY, inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter och friheter, ska rapportering även ske till de berörda registrerade personerna, utan dröjsmål. Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till IMY samt rapportering till de berörda personerna.

3.6.3 Resultat

Riktlinje och rutiner finns för rapportering i IA och verksamhetens eget register.

Inga allvarliga incidenter finns för 2022.

3.6.4 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
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

3.6.5 DSO ger råd och rekommendationer till PUA

Inga rekommendationer.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Registerförteckning
- Styrdokument
- Infoklassning
- Konsekvensbedömning
- Registerutdrag
- Incidentrapportering

4.2 Syfte

En av dataskyddsombudets viktigaste uppgifter är att övervaka verksamhetens efterlevnad av dataskyddsförordningen. En central del av det arbetet är att göra återkommande granskningar av hur väl dataskyddsförordningen efterlevs. Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten kan fatta i fråga om dataskyddsåtgärder. För PUA är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året och vad resultaten av granskningarna är.

4.3 Genomförda granskningar och deras resultat

4.3.1 Registerförteckning

Registerförteckningen har kontrollerats mot de behandlingar som sker. Dessa har i sin tur kontrollerats genom att de som ansvarar för en viss behandling har fått ange om denna förändrats, ex genom nya typer av personuppgifter eller förändrat syfte m.m.

	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

4.3.2 Styrdokument

Styrdokumenten har granskats till innehåll samt att styrelsen har fastställt desamma under året. Vidare har informationen på bolagets hemsida kontrollerats.

	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

4.3.3 Infoklassning

Infoklassning har kontrollerats genom intervjuer med berörd personal samt granskning av dokumenterade klassningar.

Klassning har inte utförts av den information som finns i stadens centrala system. Klassning av eget verksamhetssystem (Insman) har inte uppdaterats. Behandlingen eller personuppgifterna har dock inte ändrats sedan föregående klassning.

Stadens gemensamma system har en hög säkerhet, varför information som finns i dessa har låg risk. Vidare kan verksamheten dokumentera centralt gjorda klassningar.

Av verksamheten gjorda klassningar har inte uppdaterats, men personuppgifterna har inte ändrats sedan senaste klassning.

Under 2022 har en IT-ansvarig anställt, konsult för infoklassning anlitats och infoklassningar påbörjats.

Sammantaget bedöms risken som låg.

	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

4.3.4 Konsekvensbedömningar

Kontroll har skett av upprättade konsekvensbedömningar mot innehållet i registerförteckning och gällande rätt.

Konsekvensbedömningar har identifierats till 4 st behandlingar:

a. Insman försäkrings/skadesystem
b. Belivia skadeanmälningsmodul
c. Hantering av information kring arbetstagare
d. IA (avseende arbetsskador)

Av dessa har IA ännu inte konsekvensbedömts i väntan på uppdaterad infoklassning, vilken har slutförts i slutet av 2022. De övriga har inte uppdaterats, men behandlingarna har inte ändrats sedan förra bedömningen.

IA har hög säkerhet och används av flera kommuner för ex arbetsskador, varför risken bedöms som låg.

Då IT-ansvarig anställts under 2022 och infoklassningar påbörjats kommer konsekvensbedömningar att uppdateras när klassningar slutförts.

Övriga bedömningar har inte ändrats och risken bedöms som låg.

	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 Registerutdrag

Kontroll har skett av inkomna begäran av utdrag, vilket granskats mot fört register för utdrag samt svarstider.

Begäran om registerutdrag har inte förekommit under 2022.

	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

4.3.6 Incidentrapportering

Kontroll har skett av bolagets rapportering i IA, protokoll veckomöten (incidenter är en stående punkt) samt bolagets eget incidentregister.

3 st incidenter under 2022 som avser bristande åtkomst. Risk för de registrerades rättigheter har dock inte förekommit.

	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

4.4 DSO ger råd och rekommendationer till PUA

Bolaget bör under 2023:

a) Infoklassa samtlig informationshantering enligt registerförteckningen (använda ev. centralt genomförda klassningar).
b) Uppdatera tidigare utförda infoklassningar (kan ske genom dokumentation av att förändringar inte skett)
c) Utföra konsekvensbedömning av IA efter uppdaterad klassning.
d) Uppdatera tidigare utförda konsekvensbedömningar (kan ske genom dokumentation av att förändringar inte skett).

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- Ej utförda/uppdaterade infoklassningar och konsekvensbedömningar
- Behörigheter i Insman och IA

5.2 Syfte

Verksamheten har ansvar för att göra vissa typer av riskanalyser, så som konsekvensbedömningar och informationsklassningar, men dessa ger inte en heltäckande bild av personuppgiftsriskerna i verksamheten. Dataskyddsombudet behöver som underlag för sin egen planering och sitt löpande arbete ha kontinuerlig överblick över dessa risker, i verksamhetens samtliga personuppgiftsbehandlingar. Exempelvis krävs en sådan överblick för att kunna välja ut vilka områden som bör granskas under det kommande året eller för att avgöra vilka råd som dataskyddsombudet behöver lämna till verksamheten om dataskyddsåtgärder som behöver vidtas.

5.3 Resultatet av riskkartläggningen

Riskanalys har genomförts av DSO baserat på känsligheten i de personuppgifter som behandlas, konsekvensanalys och infoklassning.

Brister i infoklassning och konsekvensbedömning kan innebära felaktig syn på riskerna med behandling/laglighet av behandling samt även synpunkter från tillsynsmyndigheten.

S.k. känsliga personuppgifter behandlas i verksamhetssystem Insman, bolagets G/-katalog hos TIETO och i AFA:s system IA. Kontroller av TIETO sker på övergripande nivå av Stockholms stad, varför bolagets risker avseende känsliga personuppgifter kan koncentreras till Insman och IA.

De risker som är förknippade med dessa system (se konsekvensbedömning Insman och infoklassning IA) är i första hand frågor kring obehörig åtkomst, infoklassning och konsekvensbedömning. Av den anledningen bör kontroller under 2023 avse dessa områden.

	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

5.4 DSO ger råd och rekommendationer till PUA

Genomför/uppdatera infoklassningar och konsekvensbedömningar, se 4.4 ovan, samt genomför kontroll av behörigheter i egna system.

6 Planerade granskningar och aktiviteter under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Obligatoriska områden enligt ovan.
- Behörigheter i Insman och IA.

6.2 Syfte

Granskningsområdena bör lämpligen väljas utifrån ett riskbaserat synsätt, det vill säga att fokus bör ligga på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Därigenom åstadkoms en röd tråd i dataskyddsarbetet från ett verksamhetsår till nästa samtidigt som de största riskerna elimineras eller åtminstone sänks till en mer acceptabel nivå.

6.3 Planerade granskningar

6.3.1 Obligatoriska områden

Se kapitel 3 för områden och 4 för kontroller.

6.3.2 Behörigheter Insman och IA

Kontrollera behörighet i systemen Insman och IA genom att administratörerna i systemen får visa vilka som har behörighet på olika nivåer efter sin respektive roll.

6.4 Årsplan 2023

Q1

- Årsrapport 2022

Q2

- Kontroll av obligatoriska områden enligt kap 3 och 4.

Q3

- Kontroll av behörighetsbegränsningar i Insman och IA
- Riskanalys för 2023

Q4

- Årsplan 2024

7 Övrigt att rapportera

Inget övrigt att rapportera eller rekommendera.