Utfallsrapport VB 2025
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: GDPR årsrapport 2025 St Erik Försäkring

Bilaga 2: SEF Personalredovisningsblankett 2025

Sammanfattande kommentar

S:t Erik Försäkrings AB ska svara för att det finns en effektiv riskfinansiering av anläggningar och verksamheter ägda av staden och närstående bolag, ge stöd till stadens nämnder och bolag i arbetet med att identifiera risker samt förebygga och minimera skadeverkan.

Bolaget har under året arbetat inom samtliga av sina områden och bedöms uppfylla de mål, indikatorer och aktiviteter som bolaget har.

Analys av ekonomisk utveckling

Resultatsammanställning, investeringar & övrigt

Resultatsammanställning

Nyckeltal	Utfall	Budget VB	Prognos
Omsättning	188 161	126 600	110 415
Rörelsekostnader	-157 372	-115 700	-103 500
Avskrivningar			
Nedskrivningar och Utrangeringar			
Personalkostnader	-14 923	-15 000	-15 000
Övriga kostnader			
Finansnetto	10 147	5 100	9 000
Resultat efter finansnetto	26 013	1 000	915

Investeringar

Nyckeltal	Utfall	Budget VB	Prognos
Nyproduktion			
Strategiska investeringar (Ombyggnad)			
Ersättningsinvesteringar			
Summa investeringar			

Övrigt

Nyckeltal	Utfall
Antal anställda	10
Balansomslutning	443 384

Åtgärdande av tidigare års rekommendationer från lekmannarevisorerna

I granskningen av årsredovisningen för 2021 fick bolaget rekommendation att säkerställa dataskyddsombudets oberoende samt att säkerställa att samtliga informationstillgångar säkerhetsklassas efter behov och minst årligen. Informationsklassningar genomförs årligen och från och med hösten 2025 har bolaget säkrat oberoendet för dataskyddsombudet genom att köpa tjänsten från serviceförvaltningen.

Analys

Den automatgenererade tabellen ger ett felaktig bild då försäkringsbolag gör sin budget enligt f e r (för egen räkning) med avdrag för återförsäkringskostnaderna och återförsäkrarnas andel av skadekostnaderna.

Enligt bolagets redovisning är ställningen som följer:

Premieintäkt f e r 110 395 (budget 126 600 tkr)

Försäkringsersättningar f e r 66 686 (budget 105 050 tkr)

	2025	2024	2023	2022	2021
Antal skador (exkl. olycksfall)	188	236	249	210	269
Skadekostnad, mnkr (exkl. olycksfall)	49	39	96	45	86
Resultat före bokslutsdispositioner och skatt, mnkr	26,0	44,9	-2,7	17,1	-14,3

Bolagets resultat före bokslutsdispositioner och skatt för perioden var 26,0 mnkr och beror på lägre skadekostnader än budgeterat, trots att antalet skador var i nivå med föregående års. Det är alltid en eftersläpning i rapporteringen av skador, därför kommer antalet skador för 2025 att revideras upp. Vid en jämförelse med 2024 var resultatet 44,9 mnkr som en följd av låga skadekostnader. I tabellen ovan är skador inom olycksfall exkluderat. Tabellen tydliggör att bolagets skadekostnader är mycket volatila och påverkar bolagets ekonomi till mycket stor del. Det är tydligt att skadekostnaderna fluktuerar kraftigt mellan åren.

Bedömning av bolagets interna kontroll

Bolaget bedömer att den interna kontrollen under år 2025 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. Ett Stockholm som håller samman med en stark och jämlik välfärd i hela staden

1.1 Alla barn och ungdomar ska ges möjlighet till jämlika uppväxtvillkor och trygghet samt en rik fritid

Ej relevant för S:t Erik Försäkrings AB.

1.2 Alla barn ska ges likvärdig möjlighet till utveckling och lärande i förskolan och skolan

Ej relevant för S:t Erik Försäkrings AB.

1.3 Stockholms stad ska ge stöd och omsorg där behoven är som störst

S:t Erik Försäkrings bidrag avseende att säkerställa rättigheter för personer med funktionsnedsättning sker främst genom att tillhandahålla försäkringslösningar för förvaltningar, bolag, arbetssökande, praktikanter och elever i stadens verksamheter eller externt. Vidare säkerställer också S:t Erik Försäkring att bolagets webbplats är tillgänglighetsanpassad, i enlighet med EU-direktiv och lagstiftning på området.

1.4 Stockholm ska vara en bra stad att åldras i - med god omsorg och stor trygghet

Ej relevant för S:t Erik Försäkrings AB.

1.5 Alla stockholmare ska ha tillgång till ett rikt kultur-, idrotts- och föreningsliv

S:t Erik Försäkrings bidrag avseende att säkerställa Stockholms stads program för idrott, motion och friluftsliv 2024-2028 sker främst genom att tillhandahålla försäkringslösningar för förvaltningar, bolag, arbetssökande, praktikanter och elever i stadens verksamheter eller externt.

2. Ett grönt och fossilfritt Stockholm som leder en rättvis klimatomställning

2.1 Stockholm ska bli klimatpositivt – genom minskade utsläpp och ökad koldioxidlagring

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
I samverkan med stadens nämnder och bolagsstyrelser och i samråd med Storstockholms brandförsvar stärka det förebyggande strategiska arbetet för att minska antalet brand- och vattenskador samt begränsa konsekvenserna av dessa.				Stärka det förebyggande strategiska arbetet för att minska antalet brand- och vattenskador genom det doktorandprojekt tillsammans med KTH som påbörjades under 2024 och som syftar till att minska antalet frekvens- och klimatrelaterade skador för stadens bostadsbolag. **Analys** Arbetet har genomförts i enlighet med målsättning. Ingen avvikelse finns att rapportera.

2.2 Stockholm ska vara en stad där den biologiska mångfalden ökar

S:t Erik Försäkring bidrar till måluppfyllelse av kommunfullmäktiges mål genom att samarbeta med förvaltningar och bolag avseende skyfalls- och värmekarteringar och låta dessa få genomslag i både premiesättning och villkor. Det skapar incitament vid planering- och produktion av byggnader.

2.3 Stockholm ska vara en stad där framkomligheten ökar och utsläppen minskar

S:t Erik Försäkring bidrar till stadens arbete inom området genom att tillhandahålla eller förmedla adekvata försäkringslösningar samt rådgivning avseende krav på försäkring i entreprenader. Vidare har bolaget en resepolicy som reglerar bolagets verksamhet för att bidra till minskade utsläpp.

2.4 Stockholmarnas hälsa ska främjas genom ren luft, rent vatten och giftfria miljöer

Ej relevant för S:t Erik Försäkrings AB.

3. Ett Stockholm med en stabil och hållbar ekonomi med utbildning, jobb och bostäder för alla

3.1 Stockholms ekonomi är stark, hållbar och lägger grunden för en jämlik välfärd

S:t Erik Försäkring fortsätter att arbeta för att effektivisera verksamheten. Arbetet i företaget ska bedrivas så kostnadseffektivt som möjligt inom ramen för vad bolagets övriga mål tillåter. Bolagets rutiner ses kontinuerligt över för att om möjligt hitta nya metoder och hjälpmedel som kan öka effektiviteten och hålla de administrativa kostnaderna låga. En ökad grad av digitalisering kan vara en möjlig väg samt att dela funktioner med andra bolag. Under 2025 har bolaget infört en "min-sida" för vårdnadshavare/skadelidande inom olycksfallsförsäkringen.

S:t Erik Försäkring delar lokaler med Stockholmsregionens Försäkring AB (SRF). Vidare delar S:t Erik Försäkring IT-ansvarig med SGA Fastigheter, S:t Erik Markutveckling och moderbolaget. Bolaget har även ett nära samarbete med övriga kommunalt ägda försäkringsbolag i Sverige avseende upphandling m.m. Möjligheten att dela ytterligare funktioner med andra bolag ses löpande över.

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
Ansvara för att prioritera, driva och säkerställa innovation och digitalisering internt samt främja närliggande externa aktörers innovationsförmåga				Genomföra utbildning och ta fram förslag på användningsområden inom bolaget där AI kan bidra till att effektivisera eller utveckla verksamheten. **Analys** Utbildning har genomförts och ett projekt angående skadedata har genomförts.

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
				Utveckla en "min sida" för olycksfallsskador i bolagets försäkringssystem. **Analys** Under mars månad infördes "min sida" för olycksfallsskador i bolagets försäkringssystem.
Arbeta för att öka extern finansiering				Genomföra doktorandprojekt som delfinansieras tillsammans med KTH under perioden 2024-2026 i syfte att minska antalet frekvens- och klimatrelaterade skador för stadens bostadsbolag. **Analys** Arbetet har genomförts i enlighet med målsättning. Ingen avvikelse finns att rapportera.
Genom premiesättning säkerställa att skademinimerande och riskförebyggande arbete premieras				Anpassa priset på försäkringsskydden så att skadeförebyggande, riskförebyggande och klimatförebyggande arbete premieras **Analys** Arbetet har genomförts i enlighet med målsättning. Ingen avvikelse finns att rapportera.
Medverka till 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**	100	100 %	
	Samtliga försäkringstagare ska erbjudas ett årligt förnyelsebesök. **Analys**	100	100 %	
Optimera den				Årlig

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
försäkringsrisk som bolaget själv tar i förhållande till fastslagen risknivå				sammanfattande rapport till kommunkoncernen. **Analys** Arbetet har genomförts i enlighet med målsättning. Ingen avvikelse finns att rapportera.
Stödja det olycks- och skadeförebyggande arbetet i kommunkoncernen	Antalet genomförda riskbesiktningar (sammantaget byggnader och verksamheter) **Analys**	100	80	
	Antalet incidenter som rapporteras i stadens incidentrapporteringssystem. **Analys**	29 329	18 000	
				Analys av incidenter i IA, skadestatistik, riskbesiktningar, SBA, omvärldsbevakning samt dialog med kunderna. **Analys** Arbetet har genomförts i enlighet med målsättning. Ingen avvikelse finns att rapportera.
	Andel administrations- och indirekta kostnader **Analys**	24,5 %	26 %	
	Avvikelse investeringsbudget, % **Analys**	0 %	0 mnkr	
	Driftskostnader i förhållande till premier för egen räkning **Analys**		26 %	
	Resultat efter finansnetto(mnkr) **Analys**	26	1	

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
	SCR-kvot **Analys**	4,7	1,5	

3.2 I Stockholm ska alla ges möjlighet till ett eget jobb

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

S:t Erik Försäkrings bidrag avseende näringslivspolicyns fokusområden sker främst genom att tillhandahålla försäkringslösningar för förvaltningar, bolag, arbetssökande, praktikanter och elever i stadens verksamheter eller externt.

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
I ökad utsträckning tillgängliggöra arbetsplatser genom sociala krav i stadens upphandlingar				
	Antal tillhandahållna platser för feriejobb **Analys**	0 st	0 st	
	Antal tillhandahållna platser för Stockholmsjobb **Analys**	0 st	0 st	

3.3 I Stockholm ska alla ha rätt till ett bra boende som de har råd med

Ej relevant för S:t Erik Försäkrings AB.

3.4 Medarbetare i Stockholm ska ges goda förutsättningar att göra ett bra jobb

S:t Erik Försäkring har en liten organisation med 9 st anställda. Samtliga är specialister med kvalificerad utbildning och många års erfarenhet. Tjänsterna utformas i samverkan med VD och personalen har en mycket stor möjlighet till påverkan på tjänsternas utformning. VD styr tillitsbaserat där personalen själva lägger upp arbetets utformning och VD stöttar och följer upp. Utbildning är inom försäkringsbranschen lagstadgat och personalen vidareutbildas kontinuerligt i samråd med VD. Varje år genomgår nyckelbefattningar, inkl. VD, test av kunskaperna.

Arbetsmiljö är en stående fråga vid varje APT samt följs upp och dokumenteras av VD och facklig företrädare.

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
Arbeta för att stadens medarbetare inte utsätts för hot, rasism eller otillbörlig påverkan				Säkerställa att policys och program avseende hot, rasism eller otillbörlig påverkan är uppdaterade. **Analys** Arbetet har genomförts i enlighet med målsättning. Ingen avvikelse finns att rapportera.
	Aktivt Medskapandeindex **Analys**	98	85	
	Sjukfrånvaro **Analys**	0,5 %	2,5 %	
	Sjukfrånvaro dag 1-14 **Analys**	0,5 %	2,5 %	
				S:t Erik Försäkring ska vidareutveckla arbetet med att skapa möjligheter till ett flexibelt och långsiktigt hållbart arbetsliv i syfte att attrahera, utveckla och behålla medarbetare. **Analys** Arbetet har genomförts i enlighet med målsättning. Ingen avvikelse finns att rapportera.

3.5 Hög beredskap och stark rådighet ska råda i alla verksamhetsområden

S:t Erik Försäkring lyder under försäkringsrörelselagen och de riktlinjer som Finansinspektionen utfärdar. Vidare omfattas bolaget av ett stort antal EU-förordningar för just försäkringsbolag. Regelverket är omfattande avseende intern styrning och kontroll. Bolagets interna kontroll har därför utformats i enlighet med dessa regelverk och återfinns i flertalet av bolagets riktlinjer.

Bolagets organisation avseende riskhantering är organiserat med, för försäkringsbolag, lagstadgade centrala funktioner (riskhanteringsfunktion, regelefterlevnadsfunktion, internrevision samt aktuarie) samt därutöver

ISAM och DO.

På informationssäkerhetsområdet finns särskilda regler för försäkringsbolag som inte omfattar staden i övrigt, EBA:s riktlinje GL/2019/02, EIOPA 20-002, Eiopas riktlinjer (20/600) för säkerhet och företagsstyrning avseende IKT.

Informationssäkerhetsrisker hanteras således av verksamheten med stöd av riskhanteringsfunktionen, ISAM, DSO och IT-ansvarig. Arbetet sker löpande och granskas av riskhanteringsfunktionen, regelefterlevnadsfunktionen, ISAM, DSO samt internrevisionen. Rapportering sker, som för andra risker, av riskhanteringsfunktionen till styrelsen vid varje styrelsemöte eller behov. DSO avlägger årligen egen rapport.

Vad avser RSA hanteras dessa risker av verksamheten i samarbete med bolagets ovan beskrivna riskhanteringsfunktion. Varje risk har en riskägare och åtgärdsplan (såvida inte risken accepteras). Riskhanteringsfunktionen rapporterar risknivåer, riskhantering m.m. till styrelsen vid varje styrelsemöte samt vid behov. Riskhanteringsfunktionens arbete kontrolleras av internrevisionen.

Bolaget deltar aktivt i arbetet med civil beredskap inom finansiell beredskap.

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
Bistå stadens förvaltningar och bolag med att identifiera sina oönskade risker ur ett försäkringsperspektiv.				Genomföra riskbesiktningar, utbilda och stödja stadens enheter i SBA, tillhandahålla incidentrapporteringssystem och skadestatistik. omvärldsbevaka och ha löpande dialog med kunderna. **Analys** Arbetet har genomförts i enlighet med målsättning. Ingen avvikelse finns att rapportera.
	Andel prioriterade avtal där uppföljning genomförts **Analys**	100 %	100 %	Införa regelverket för digital operativ motståndskraft för finanssektorn (DORA) **Analys** Arbetet har genomförts i enlighet med målsättning. Ingen avvikelse finns att rapportera.
				Följa färdplan informationshantering **Analys** Arbetet har genomförts i enlighet med målsättning. Ingen avvikelse finns att rapportera.
				Följa lagar, regler och förordningar genom strukturerade processer och god egenkontroll.

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
				Analys Arbetet har genomförts i enlighet med målsättning. Ingen avvikelse finns att rapportera.

3.6 Tryggheten ska öka genom förebyggande insatser

Som försäkringsbolag omfattas S:t Erik Försäkring av regelverket för försäkringsbolag och står under Finansinspektionens tillsyn. Som ett led i detta finns fyra särskilda kontrollfunktioner, riskhanteringsfunktion, internrevision, aktuarie och regelefterlevnadsfunktion. Funktionerna granskar och kontrollerar bolaget, vilket redovisas i rapport till styrelsen vid varje styrelsemöte. Bolaget genomför även uppföljning av leverantörer, vilket också granskas av funktionerna. Dessa regelverk och kontrollfunktioner är en viktig del i bolagets arbete för att motverka välfärdsbrott.

Bolagsstyrelsens mål för verksamhetsområdet	Indikator	Periodens utfall	Årsmål	Aktivitet
Med stöd i lokal lägesbild och analys vidta sociala och situationella brottsförebyggande och trygghetsskapande åtgärder utifrån det egna ansvarsområdet				

3.7 Stockholm ska vara en öppen, jämställd och demokratisk stad som samarbetar internationellt

S:t Erik Försäkring bidrar till målen främst genom tillhandahållande av försäkringar för förvaltningar och bolag som möjliggör deras arbete. Detta möjliggör för fastighetsägare att tillgängliggöra lokaler och för enskilda att delta i olika evenemang. Vidare tillhandahålls olycksfallsförsäkring för elever m.fl. vilket utjämnar skillnader mellan barn i familjer med olika ekonomiska förutsättningar. Vid rekryteringar främjas om möjligt en blandning av människor med olika ursprung och kön.

Verksamheten utgörs av tillhandahållande av försäkringsskydd, vilket är reglerat enligt Försäkringsrörelselagen och Försäkringsavtalslagen. Bolaget står under Finansinspektionens tillsyn. De kunder bolaget har utgörs av bolag och förvaltningar samt olycksfallsförsäkring för elever m.fl. Uppföljning av skadereglering sker genom skaderevision utfört av externt bolag. Verksamhetens reglering, art och omfattning innebär att försäkringsskyddet och tillhörande skadereglering är neutralt oavsett kön, etnicitet, könsidentitet, sexuell läggning etc.

Övrigt

CSRD/Klimathandlingsplan

Implementering av EUs direktiv för hållbarhetsrapportering, CSRD, pågår i Stadshus AB:s koncern. Tidplanen för första rapportering har förlängts till 2027, men arbetet inom koncernen fortsätter under tiden. Under året har bolaget deltagit i de samverkansgrupper som moderbolaget anordnat. Vidare har bolaget

deltagit i arbetsgrupper för att ta fram avgränsningar, tolkningar och information gällande de upplysningar som ska rapporteras enligt CSRD och EU-taxonomin. Sammanfattningsvis har arbetet präglats av ett fokuserat förberedelsearbete inför kommande CSRD-rapportering.

Under februari 2026 genomförs beräkningar av klimatutsläpp i Scope 1, 2 och 3. Dessa beräkningar avser år 2025 men enligt anvisningarna ska ingen rapportering göras i samband med den sedvanliga rapporteringen i samband med verksamhetsberättelsen.

Systematiskt kvalitetsarbete

S:t Erik Försäkring fortsätter att arbeta för att effektivisera verksamheten. Arbetet i företaget ska bedrivas så kostnadseffektivt som möjligt inom ramen för vad bolagets övriga mål tillåter. Bolagets rutiner ses kontinuerligt över för att om möjligt hitta nya metoder och hjälpmedel som kan öka effektiviteten och hålla de administrativa kostnaderna låga. Bolaget delar funktioner med andra bolag. Under 2025 har bolaget infört en "min-sida" för vårdnadshavare/skadelidande inom olycksfallsförsäkringen. Vidare har bolaget under året genomfört ett digitaliseringsprojekt avseende premieberäkning och skadedata. Bolaget har även ett nära samarbete med övriga kommunalt ägda försäkringsbolag i Sverige avseende upphandling m.m. Möjligheten att dela ytterligare funktioner med andra bolag ses löpande över. Under 2024-2026 genomför bolaget tillsammans med KTH ett forskningsprojekt för att minska frekvens- och klimatrelaterade skador hos stadens bostadsbolag.

Stockholms stad

GDPR årsrapport

År 2025

S:T ERIK FÖRSÄKRINGS AB

GDPR årsrapport
Januari 2026

Dnr: SEF 2026/1
Utgivningsdatum: 2026-01-19
Kontaktperson: Erik Fischer

Sammanfattning

GDPR, eller dataskyddsförordningen, syftar till att skydda individers grundläggande rättigheter och friheter, med särskilt fokus på rätten till skydd av personuppgifter. I Stockholms stad är varje nämnd och styrelse ansvarig för personuppgiftsbehandlingar som sker i den egna verksamheten. Ett dataskyddsombud har i uppdrag att oberoende granska verksamhetens efterlevnad av dataskyddsförordningen. I denna rapport redovisar dataskyddsombudet årets granskning av **S:t Erik Försäkrings ABs** dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

PA har en väl utformad organisation avseende personuppgiftshantering, såväl vad avser organisation som erforderliga mallar och hantering. DSO rekommenderar att PA fortsätter att ha personuppgifter och incidenthantering som en stående punkt på PAs veckomöten samt arbetar systematisk med den pågående uppdateringen av registerförteckningen enligt vad som framgår av noteringar nedan.

De tre största riskerna enligt dataskyddsombudets bedömning

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Registerförteckning		Pågående uppdatering/revision av registret innebär en liten risk att det under arbetet kan finnas dubbel, eller bortfall, av information. Rekommendation att PA vid begäran av utdrag även jfr med äldre version av registret.

Innehållsförteckning

Inledning

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

I Stockholms stad är varje nämnd och styrelse ansvarig för personuppgiftsbehandlingar som sker i den egna verksamheten.

Dataskyddsombudets uppgift

Varje personuppgiftsansvarig (nämnd eller styrelse) ska utse ett dataskyddsombud. Dataskyddsombudets uppgifter framgår direkt av lagstiftningen. Ombudets roll är att kontrollera att GDPR följs inom organisationen. Det innebär bland annat att ge råd, rekommendationer och informera om frågor som rör behandlingar av personuppgifter. Dataskyddsombudet har även i uppdrag att oberoende granska verksamheternas arbete med dataskyddsfrågor för att säkerställa att dataskyddslagstiftningen efterlevs. DSO ska rapportera direkt till högsta förvaltnings-/bolagsnivå. I Stockholms stad innebär det att dataskyddsombudet rapporterar till nämnder och styrelser.

Dataskyddsombudet lämnar årligen en rapport om verksamhetens dataskyddsarbete till varje nämnd och styrelse. Genom rapporten kan nämnd och styrelse ta emot de råd och rekommendationer som dataskyddsombudet lämnar. Årsrapporten syftar till att nämnd/styrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Årsrapporten är ett medel för nämnds/styrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Granskning av dataskyddsarbetet 2025

Kontroll av obligatoriska områden

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

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

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

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

Resultatsammanställning från granskningen av de sex obligatoriska områdena

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

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

Register över personuppgiftsbehandlingar

Sammanfattning

Registret omfattar de behandlingar som PA utför och har en bra koppling till bolagets system och processer. Vid uppdateringar av registret rekommenderas PA att jfr ny version med äldre om begäran av registerutdrag inkommer för att säkerställa att rätt information lämnas ut.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		14
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		JA
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		JA. Registret är fn under revision och därmed finns en liten risk för att information kan dubbleras eller falla bort. PA har en god kontroll över behandlingarna och vilket innehåll registret ska omfatta. Risken bedöms därför som liten.
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		JA

Säkerhet i samband med behandlingen

Sammanfattning

PA bedöms att efterleva gällande regelverk och ha en väl anpassad organisation för hantering av säkerhet. Infoklassningar, styrdokument är väl avpassade för verksamhetens behov.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Efter ett antal stickprov på genomförda informationsklassningar, bedömer DSO att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?		JA
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		JA
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		JA

Konsekvensbedömning avseende dataskydd

Sammanfattning

PA har en väl anpassad organisation för hantering av konsekvensbedömningar. En modernare version av mallar kan övervägas.

Behandlingar som bör konsekvensbedömas har identifierats:

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

Behandlingar a-c har konsekvensbedömts.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		JA Samtliga behandlingar granskas minst årligen eller vid förändring avseende behovet av konsekvensbedömning. PA har personal som genomgått certifieringsutbildning DSO.
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		JA Samtliga behandlingar granskas minst årligen eller vid förändring avseende behovet av konsekvensbedömning.
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		JA Mall finns och har använts regelbundet. PA kan överväga att modernisera mallen, dock förligger inte någon risk att konsekvensbedömning utförs felaktigt med nuvarande mall.
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		JA Konsekvensbedömningar sker varje år och därutöver om det är erforderligt.

Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		JA Bolaget har sällan ändrade behandlingar och de som finns har diskuterats och kontrollerats avseende konsekvensbedömning.

Den registrerades rättigheter

Sammanfattning

PA bedöms efterleva gällande regelverk och har en väl anpassad organisation och hantering av registrerads rätigheter.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	**Risk**	**Rekommendationer**
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		JA PA har riktlinje för hantering av personuppgifter med fördelat ansvar samt beskrivning av process.
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		Inga.
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		N/A
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		N/A

Personuppgiftsincidenter

Sammanfattning

PA har under året inte haft några personuppgiftsincidenter och bedöms efterleva gällande regelverk.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	**Risk**	**Rekommendationer**
Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident?		I PAs Riktlinjer för hantering av personuppgifter framgår ansvar och incidenthantering
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		JA PA har styrdokument för incidentrapportering där rutiner och processer framgår: • Riktlinje för hantering av personuppgifter • Hanteringsrutin för informationssäkerhetsincidenter • IKT riktlinje • Lokal anvisning för informationssäkerhet • Riktlinje för incidenthantering
Hur många personuppgiftsincidenter har dokumenterats under året?		Inga.
Hur många personuppgiftsincidenter har anmälts till IMY under året?		Inga

Överföring till tredje land

Sammanfattning

PA bedöms efterleva gällande regelverk och har processer för att hantera eventuella överföringar till tredje land.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		Pa har bara ett eget system (skade och försäkringssystemet Insamn) hos extern leverantör. Där förekommer inte tredjelandsöverföring. Vad avser stadens system som PA är en del av får frågan ställas till SLK IT.
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		N/A
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		N/A

Resultatsammanställning från övriga granskningar

Behörighetsstyrning i verksamhetssystem

Under året har en uppföljning av behörighetsstyrning av verksamhetssystem gjorts. Bolaget har en generell rutin för behörighetstilldelning samt avslut av behörigheter i system. Bolaget följer även årligen upp behörigheter i olika system, vissa högrisksystem följs upp med större frekvens. Vid kontroll hade samtliga system en dokumenterad senast uppföljning av behörigheter. Generellt arbetar bolaget mycket väl med behörighetsstyrning. Vissa verksamhetssystem skulle dock behöva definiera hur ofta

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig rutiner för tilldelning av behörigheter i verksamhetssystem?		JA För det egna systemet Insman hanterar systemansvarig detta regelbundet. För stadsgemensamma system hanterar PA ISAM detta regelbundet.
Har personuppgiftsansvarig rutiner för avslutande av behörigheter i verksamhetssystem?		JA PA har få anställda, 9 st, och en personalomsättning de senaste åren på 0%. PA har således en mycket bra kontroll på avslut av behörigheter.

Bilagor

Bilaga 1: Detaljerad redovisning av dataskyddsombudets granskning

Bilaga 2: Andra genomförda granskningar och omvärldsbevakning

Bilaga 1 - Detaljerad redovisning av dataskyddsombudets granskning

Denna bilaga innehåller en beskrivning av syftet med respektive obligatoriskt område samt en mer detaljerad redovisning av dataskyddsombudets granskning och slutsatser. Här framgår vilka iakttagelser som gjorts och vilken information som samlats in under granskningsarbetet av de sex obligatoriska rapporteringsområdena. För varje område redovisas de underlag som har använts, de iakttagelser som har gjorts samt hur dessa har utgjort grunden för dataskyddsombudets riskbedömning och rekommenderade åtgärder.

1. Register över personuppgiftsbehandlingar

Syftet med området

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

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

Kontroller och iakttagelser gjord av dataskyddsombudet

Antal behandlingar som är registrerade?

14. Kontroll har skett genom jfr mellan register och infoklassningar.

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

Ja. Registret är strukturerat och ansvarig är certifierad, Riktlinjer finns som omfattar förändringar av registret.

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

Ja. F.n. pågår en uppdatering av registret, vilket innebär en lite risk för felaktigheter. Dessa bedöms inte påverka de registrerades rättigheter.

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

Ja. Kontroll av registret.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Den pågående uppdateringen av registret innebär en liten risk för att felaktigheter kan förekomma under revisionstiden. Med anledning av PA s riktlinjer och medvetenhet bedöms dock risken som lite.

Dataskyddsombudets bedömning samt rekommendationer

Registerförteckningen uppfyller kraven enligt gällande regelverk.

En liten risk för felaktigheter vid den pågående uppdateringen av registret föreligger. PA rekommenderas att vid begäran om registerutdrag kontrollera både den nuvarande samt äldre versionen av registret för att minimera felaktigheter.

2. Säkerhet i samband med behandlingen

Bakgrund och syfte

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

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

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

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

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

informationsklassningar och riskanalyser. Vidare bedömer DSO huruvida det finns tillräckligt mycket reglerat om dataskydd i styrdokument och rutiner samt om dessa är tillräckligt implementerade och kända.

Kontroller och iakttagelser gjord av dataskyddsombudet

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

Ansvarig hos PA (DSO vid tiden för klassningarna) arbetar i systemen och har deltagit i samtliga infoklassningar, vilka innehåller det som behövs.

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

PA omfattas som försäkringsbolag av DORA-förordningen (EU 2022/2554) om digital operativ motståndskraft och har ett stort antal styrdokument som reglerar inte bara personuppgifter, utan även IT-säkerhet. Styrdokumenten innehåller den information och beskrivning av processer som är erforderliga för ett bolag under Finansinspektionens tillsyn.

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

PA är ett litet bolag med få anställda där flera av de anställda, samt regelefterlevnadsfunktionen, har deltagit i framtagande av dokument och där infosäkerhet är fråga som diskuteras regelbundet. Vid veckomöten är dessutom frågan om incidenter en stående punkt.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Nej. PA har samma behandlingar som tidigare år med samma personuppgifter.

Dataskyddsombudets bedömning samt rekommendationer

Organisationen är väl insatt i behandlingarna och IT-säkerhet, personuppgiftsbehandling m.m. diskuteras regelbundet. Ansvarig hos PA för personuppgifter arbetar dessutom i systemen och har full insikt i behandlingarna.

3. Konsekvensbedömning avseende dataskydd

Bakgrund och syfte

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

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

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

Syftet med detta rapporteringsområde är att rapportera huruvida verksamheten har ändamålsenliga rutiner som möjliggör att tröskelanalyser och konsekvensbedömningar genomförs, huruvida sådana genomförs när det krävs samt huruvida personuppgiftsansvarig har genomfört konsekvensbedömningar för de behandlingar som kräver det.

Kontroller och iakttagelser gjord av dataskyddsombudet

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

Ja, både i form av riktlinjer, processer och medvetenhet.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

JA. Bolagets behandlingar är oförändrade år efter år. Försäkringsverksamheten är starkt reglerad av såväl svensk- som EU-lagstiftning och bolagets verksamhet har inte ändrats. Vid en eventuell ny behandling kontrolleras denna och dokumenteras i PAs mallar för behandlingar och då görs även kontroll av behovet av konsekvensbedömning.

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

JA

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

JA

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

JA

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Nej. PAs verksamhet är oförändrad och utförs i samma system som året före. Den hantering av personuppgifter som behövs för verksamheten har inte förändrats, behandlingarna och deras innehåll är oförändrat.

Dataskyddsombudets bedömning samt rekommendationer

PA har erforderliga mallar och hantering av konsekvensbedömningar.

4. Den registrerades rättigheter

Bakgrund och syfte

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

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

Kontroller och iakttagelser gjord av dataskyddsombudet

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

JA. Mallar för svar och påföljande info om registrerads rättigheter finns och har använts. Rutiner finns beskrivna och PAs ansvarig för personuppgifter har själv upprättad mallar och rutiner.

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

Inga. Generellt får bolaget endast begäran vid massutskick till stadens samtliga förvaltningar och bolag.

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

Inga inkomna under 2025. Historiskt har svar skickats omgående.

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

Ja. 2025 har ingen begäran om registerutdrag inkommit. Historisk har begäran besvarats omgående i enlighet med de mallar PA har och info om registrerads rättigheter bilagerats svaret.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Nej.

Dataskyddsombudets bedömning samt rekommendationer

Pa efterlever väl aktuellt område.

5. Personuppgiftsincidenter

Bakgrund och syfte

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

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

Om en personuppgiftsincident inte bedöms vara anmälningspliktig ska den dokumenteras.

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

Kontroller och iakttagelser gjord av dataskyddsombudet

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

I PAs Riktlinjer för hantering av personuppgifter framgår ansvar och incidenthantering. Incidenter och frågor kring detta behandlas även vid samtliga veckomöten och vid behov däremellan.

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

JA

PA har styrdokument för incidentrapportering där rutiner och processer framgår:

- Riktlinje för hantering av personuppgifter
- Hanteringsrutin för informationssäkerhetsincidenter
- IKT riktlinje
- Lokal anvisning för informationssäkerhet
- Riktlinje för incidenthantering

Som beskrivits tidigare behandlas frågor kring incidenter vid varje veckomöte och frågan om personuppgifter är en regelbunden fråga i organisation, inte minst med anledning av verksamhetens omfattande regelverk för försäkringsbolag och IT-säkerhet.

Hur många personuppgiftsincidenter har anmälts till IMY under året?

Inga.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Nej.

Dataskyddsombudets bedömning samt rekommendationer

Pa har en dokumenterad och implementerad process för hantering av incidenter och bedöms efterleva området.

6. Överföring till tredje land

Bakgrund och syfte

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

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

Kontroller och iakttagelser gjord av dataskyddsombudet

Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?

PA har kontrollerat sin leverantör av verksamhetssystemet Insman där tredjelandsöverföringar inte sker. I övrigt använder PA stadens system där kontroller sker av staden.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

Ja om det är aktuellt används stadens verktyg.

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

N/A då inga överföringar sker i PAs verksamhetssystem.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Nej.

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

Dataskyddsombudets bedömning samt rekommendationer

PA bedöms efterleva gällande regelverk.

Bilaga 2 – Andra genomförda granskningar och omvärldsbevakning

Andra granskningar som dataskyddsombudet har genomfört under året

Genomförda granskningar och deras resultat

Granskning av behörighetsstyrning

Under året har en granskning genomförts av behörighetsstyrning i PAs verksamhetssystem genom. Endast de som deltar i handläggningen av försäkring och skador har tillgång till systemet. Skaderegleringen hanteras genom uppdragsavtal och endast de hos leverantören som hanteras skador för PA har behörighet till systemet.

Dataskyddsombudets rekommendationer baserat på iakttagelserna ovan

Dataskyddsombudets rekommendationer
1. PA rekommenderas att fortsätta att hantera behörighetsstyrningen på det sätt som sker.

Omvärldsbevakning

Resultatet av dataskyddsombudets omvärldsbevakning

PA lyder som försäkringsbolag under en omfattande rättslig reglering. En del av det är 4 lagstadgade funktioner, regelefterlevnadsfunktion, aktuarie, internrevision och riskhanteringsfunktion som utförs av externa leverantörer. Dessa funktioner granskar bl.a. bolagets följsamhet avseende personuppgifter, men även nya och ändrade regler, vilket även rapporteras till styrelsen.

PA följer även förändringar inom personuppgiftsområdet.

Övrigt att rapportera

Inga övriga observationer