Stockholms stad

GDPR Årsrapport

År 2023

Mässfastigheter
i Stockholm AB

GDPR årsrapport
Januari 2024

Dnr:
Utgivningsdatum: 2024-01-15
Kontaktperson: Katarina Nyquist

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 lämnar jag följande årsrapport.

Stockholmsmässans dataskyddsarbete har under året fungerat väl. De nya rutiner och processer som sattes upp under 2022 har satt sig i organisationen och har fortsatt att utvecklas av den nya förvaltningsgruppen. Jämfört med rapporten förra året är det i huvudsak två områden som är värda att lyfta fram:

På Stockholmsmässan genomfördes under 2023 stickprovskontroller för sammanlagt fyra arrangemang, där samtliga affärsområden var representerade. Det var inte känt för arbetsgrupperna i förväg vilka event som skulle granskas.

Min slutsats efter stickprovskontrollerna var att arbetsgrupperna för samtliga fyra event hade skött hanteringen av personuppgifter väl. De avvikelser som noterades var samtliga av mindre allvarlig karaktär och berodde i de flesta fall på omsättning av medarbetare i arbetsgrupperna.

Under 2023 upptäcktes två personuppgiftsincidenter som beskriv närmare nedan. Ingen av dessa var av sådan karaktär att de ansågs behöva rapporteras till IMY. Båda personuppgifterna upptäcktes snabbt och hanterades enligt fastlagda rutiner.

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?	78
Har nödvändiga uppdateringar gjorts?	Ja
Bedöms registerförteckningen vara fullständig?	Ja
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

Registerförteckningen är en översikt över de olika typer av personuppgifter som Stockholmsmässan behandlar. Av förteckningen framgår bland annat vilken slags behandling som görs med uppgifterna, varifrån de kommer, var och hur länge de lagras, samt vilken rättslig grund respektive behandling vilar på.

3.1.3 Resultat

Inom Stockholmsmässan är det förvaltningsledaren GDPR som ansvarar för att gå igenom registerförteckningen årligen och göra nödvändiga uppdateringar. Till sin hjälp har denne en förvaltningsgrupp med representanter från olika delar av organisationen.

Stockholmsmässan har gjort en genomgång av samtliga personuppgiftsbehandlingar och uppdaterat registerförteckningen. Inga nya typer av behandlingar hade tillkommit. Vissa IT-system och leverantörer av IT-system hade förändrats vilket föranledde uppdateringar.

Totalt innehåller den uppdaterade registerförteckningen 78 olika behandlingar. Förteckningen bedöms vara komplett.

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

Registerförteckningen bedöms vara komplett och uppdaterad.

3.1.5 DSO ger råd och rekommendationer till PUA

Följ upp att förvaltningsledaren fortsätter att uppdatera registerförteckningen minst en gång per år, så som beskrivs i uppdraget.

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

Styrdokumenten ska ge stöd till Stockholmsmässan om hur dataskyddsarbetet ska bedrivas framför allt för två grupper: dels det som gäller förvaltningsgruppen och dels det som gäller samtliga medarbetare.

3.2.3 Resultat

Inom Stockholmsmässan är det förvaltningsledaren GDPR som ansvarar för att hålla styrdokumenten uppdaterade, och vid behov lyfta mer omfattande ändringsbehov till styrgruppen. Till sin hjälp har denne en förvaltningsgrupp med representanter från olika delar av organisationen.

Under 2023 har endast mindre förändringar gjorts i processer och rutiner gällande GDPR som krävt förändringar i styrdokumenten.

Existerande styrdokument bedöms vara kompletta och håller en lämplig kvalitet.

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

Följ upp att förvaltningsledaren är beredd att uppdatera styrdokument om förändringar skulle göras i processer och rutiner, så som beskrivs i uppdraget.

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?	75% av registerförteckningens totala antal behandlingar, samt 100% av de mest skyddsvärda behandlingarna, har informationsklassats.
Är klassade personuppgiftsbehandlingar aktuella?	Ja. Informationsklassning utförd 2022. Förnyad klassning är planerad att utföras under 2024.

3.3.2 Syfte

De tekniska och organisatoriska skyddsåtgärder som Stockholms-mässan vidtar ska säkerställa att de personuppgifter som behandlas har ett adekvat skydd mot till exempel stöld, intrång och förvanskning.

För att kunna välja rätt skyddsåtgärder måste man göra en informationsklassning av sina personuppgiftsbehandlingar. Klassningen är inte en separat aktivitet utan utgör en del av den klassning som har gjorts av Stockholmsmässans totala informationstillgångar, alltså även de tillgångar som inte innehåller personuppgifter.

3.3.3 Resultat

Stockholmsmässan vidtar de tekniska- och organisatoriska skyddsåtgärder som är tillräckliga för att säkerställa en lämplig skyddsnivå i syfte att minimera informationssäkerhetsrisker och därmed risker för vår affärskontinuitet samt för att säkerställa efterlevnad av lagar och förordningar avseende dataskydd/personuppgiftsbehandling. Skyddsåtgärderna är dokumenterade i ett specifikationsdokument som underhålls löpande.

Informationsklassning sker enligt Ledningssystem Informationssäkerhet – Lokal anvisning vartannat år eller oftare vid behov.

Senaste klassning genomfördes 2022. Förnyad klassning är planerad att utföras under 2024. Ca 75% av registerförteckningens totala antal behandlingar bedöms göras inom klassade informationstillgångar. 100% av registerförteckningens mest skyddsvärda behandlingar, och som omfattar den absoluta majoriteten av personuppgifter, bedöms göras inom klassade informationstillgångar.

I den handlingsplan som följde på klassningen 2022 har med några få undantag samtliga åtgärder genomförts. Av undantagen bedöms brister relaterade till specifikt personuppgiftsbehandling vara försumbara.

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

3.3.5 DSO ger råd och rekommendationer till PUA

Följ upp att förnyad informationsklassning genomförs planenligt och att beslutade åtgärder följs upp enligt beslutad rutin i Ledningssystem Informationssäkerhet – Lokal anvisning.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Inte aktuellt
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Inte aktuellt
Är de genomförda bedömningarna aktuella?	Inte aktuellt

3.4.2 Syfte

Om en verksamhet planerar att starta en personuppgiftsbehandling som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska man, innan behandlingen påbörjas, göra en så kallad konsekvensbedömning.

3.4.3 Resultat

Med undantag för hälsouppgifter om den egna personalen, och uppgifter om allergier i samband med matbeställningar, behandlar Stockholmsmässan aldrig några känsliga personuppgifter.

Inför införandet av GDPR 2018 gjorde man en genomgång av samtliga personuppgiftsbehandlingar och konstaterade att inga av dessa var av karaktären att de sannolikt skulle kunna leda till en hög risk för fysiska personers rättigheter och friheter.

Sedan dess har inga nya typer av behandlingar tillkommit som gett anledning att ändra detta ställningstagande, varför inga konsekvens-bedömningar har genomförts.

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

Inga konsekvensbedömningar har genomförts under året, och inga har heller behövt göras.

3.4.5 DSO ger råd och rekommendationer till PUA

Var beredda att kunna genomföra konsekvensbedömningar i framtiden, om Stockholmsmässans verksamhet skulle förändras så att den omfattar potentiella högriskbehandlingar av personuppgifter.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	20
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	19

3.5.2 Syfte

Enligt GDPR har en registrerad person rätt att vända sig till Stockholmsmässan och begära att till exempel få veta vilka personuppgifter som finns om honom eller henne (så kallat registerutdrag), korrigera felaktiga uppgifter eller i vissa fall få sina uppgifter raderade. En sådan begäran ska hanteras inom 30 dagar.

3.5.3 Resultat

Inom Stockholmsmässan är det förvaltningsledaren GDPR som ansvarar för att inkomna personuppgiftsärenden hanteras korrekt och inom 30 dagar.

Under 2023 kom det in sammanlagt 20 personuppgiftsärenden till Stockholmsmässan. 19 av dessa hanterades inom 30 dagar, ett ärende drog över ytterligare några dagar pga personalbyte. De registrerade ville göra en så kallad ”total opt-out”, det vill säga att de inte önskade några fler marknadsföringsutskick från Stockholms-mässan. Ingen person har efterfrågat ett 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

Följ upp att förvaltningsledaren fortsätter att säkerställa att rutinerna för att hantera individernas rättigheter sköts korrekt, så som beskrivs i uppdraget.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Misstänkta incidenter kan rapporteras av samtliga medarbetare via ett formulär på intranätet
Hur många personuppgiftsincidenter har dokumenterats?	2
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	0 till IMY 2 till berörda personer
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Inte aktuellt

3.6.2 Syfte

Hanteringen av eventuella personuppgiftsincidenter är en viktig och obligatorisk komponent inom GDPR för att åstadkomma en sund personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment: dokumentering och rapportering.

3.6.3 Resultat

På Stockholmsmässan kan alla medarbetare rapportera in misstänkta personuppgiftsincidenter via ett formulär på intranätet.

En förutsättning för att detta arbetssätt ska fungera är att medarbetarna är medvetna om att formuläret finns, att de är skyldiga att rapportera in misstänkta incidenter, och att de förstår varför detta är viktigt. På Stockholmsmässan finns dessa tre punkter därför med som ett inslag i den obligatoriska introduktions-utbildningen för nya medarbetare.

Under 2023 genomfördes även en repetitionsutbildning i dataskydd riktad till samtliga medarbetare (inte bara nyanställda), där information om hanteringen av personuppgiftsincidenter ingick.

Under 2023 upptäcktes två personuppgiftsincidenter som beskriv närmare nedan. Ingen av dessa var av sådan karaktär att de ansågs behöva rapporteras till IMY.

Personuppgiftsincident: Gymnasiemässan 231122

Sammanfattning av incident
Extern leverantör av Gymnasiemässans eventwebbplats. På webbplatsen registrerar sig bl a besökaren (elev/förälder) för att få biljett till eventet och får därmed tillgång till "Mina sidor". På grund av många samtidiga användare under sen eftermiddag gick webbplatsen ned dvs fungerade ej. När den var tillgänglig igen och besökare loggade på Mina Sidor för att få entrébiljett visades inte den påloggades kontaktuppgifter utan en persons för- och efternamn och mailadress visades för alla. Efter att det upptäckts korrigerades felet omgående och ingen kan efter det ha kommit åt personens uppgifter.

Påverkan
Leverantören beräknar att 154 personer har sett personens kontaktuppgifter. Personen är informerad om det inträffade.

Åtgärd
Leverantören har vidtagit åtgärder för att det inte ska kunna ske igen.

För detaljerad information hänvisas till leverantörs rapport "Sammanfattning av incident relaterat till GDPR 22 november i samband med Gymnasiemässan".

Incidenten är införd i Personuppgiftsincident loggen.

Beslut hantering
Efter att ha konsulterat IMYs hemsida bedömde förvaltningsgruppen att detta inte var en personuppgiftsincident av den allvarlighetsgrad att den måste rapporteras till IMY då personuppgifterna som offentliggjorts ej anses vara känsliga samt att det berör en person. Personen har ej skyddad identitet. Stockholmsmässan har vidtagit de åtgärder som ska ske vid en incident.

Personuppgiftsincident: Sweden Dental Expo 231120

Sammanfattning Incident
Personuppgifter från externt seminariebiljettsystem; t ex namn, email adress, företagsuppgfiter, importeras in i Stockholmsmässans biljettsystem.

Efter import av 68 biljetter med tillhörande personuppgifter 20 nov upptäckte Stockholmsmässans personal att besökarens för- och efternamn var felaktig, var en annan besökare (mailadress, företag och survey frågor är korrekt). Felet har uppstått vid manuellt handhavande av excel lista.

Påverkan
Genom tjänsten ”Lead track” kan utställare läsa av besökarens besökarbadge med en app och få uppgifter om besökaren, t ex namn, email, företag. Utställarna har fått rätt mailadress och företagsuppgifter till den besökare de läst av men fått fel för- och efternamn i 14 fall. 14st av de 68 registrerade har låtit utställare avläsa sin besökarbadge. Totalt 7 utställare har fått 1-4 felaktiga namn. 8st av de 14 besökarna har låtit en utställare läsa av sin badge. Notera att besökarens namn står på besökarens badge och är synlig för alla, ingen tidigare okänd uppgift har därmed spridits.

Åtgärd
Uppgifterna är korrigerade i biljettsystemet.Utställare är kontaktade för uppdatering av lista, för att få rätt uppgifter.

Listor som importeras in i biljettsystemet kommer att verifieras av en andra person i framtiden, innan import.

Incidenten är införd i Personuppgiftsincidentloggen.

Beslut hantering
Efter att ha konsulterat IMYs hemsida bedömde förvaltningsgruppen att detta inte var en personuppgiftsincident av den allvarlighetsgrad att den måste rapporteras till IMY då endast ett fåtal namnuppgifter, som redan var offentliga via besökarbadgen, endast visats för 1-4 utställare samt att den felaktiga personuppgiften ej anses vara känslig. Stockholmsmässan har vidtagit de åtgärder som ska ske vid en incident.

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

Fortsätt att utbilda nya medarbetare, och att påminna befintliga medarbetare regelbundet, om arbetet med personuppgiftsincidenter.

4 Genomförda granskningar under året

4.1 Sammanfattning

Stickprovskontroller för sammanlagt fyra av Stockholmsmässans arrangemang har genomförts under året. Kontrollerna visade på mindre avvikelser som har åtgärdats.

4.2 Syfte

En av dataskyddsombudets viktigaste uppgifter är att övervaka att verksamheten lever upp till bestämmelserna i GDPR. En del i detta arbete är att göra återkommande granskningar, där DSO kontrollerar hur väl förordningstexten efterlevs och ger återkoppling till verksamheten så att rätt beslut kan tas i dataskyddsfrågor.

På Stockholmsmässan genomfördes under 2023 stickprovskontroller för sammanlagt fyra arrangemang, där samtliga affärsområden var representerade. Det var inte känt för arbetsgrupperna i förväg vilka event som skulle granskas.

Vissa mindre avvikelser mot rutinerna noterades, till exempel att listor med personuppgifter inte var helt korrekt märkta, att en samarbetspartner inte fanns omnämnd på eventets webbplats, samt att några avtal med talare och moderatorer inte hade med den korrekta klausulen om personuppgiftshantering.

För ett event var det oklart om eventet hade marknadsförts till besökare vars uppgifter legat för länge i Stockholmsmässans system utifrån dataskyddspolicyn, det vill säga ifall rensningen av tidigare besökare hade utförts korrekt. Oklarheten berodde på att den medarbetare som ansvarade för rensningen våren 2023 därefter slutade på Stockholmsmässan.

Dataskyddsombudets slutsats efter stickprovskontrollerna var att arbetsgrupperna för samtliga fyra event hade skött hanteringen av personuppgifter väl. De avvikelser som noterades var samtliga av mindre allvarlig karaktär och berodde i de flesta fall på omsättning av medarbetare i arbetsgrupperna. DSO kommer att påminna Stockholmsmässans chefer om vikten av att samtliga nya

medarbetare tar del av det tillgängliga utbildnings- och informationsmaterialet.

Sammanfattande bedömning

	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 DSO ger råd och rekommendationer till PUA

Följ upp att förvaltningsledaren fortsätter att genomföra regelbundna stickprovskontroller, så som beskrivs i uppdraget.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- *Risk 1 – Listor med publika besökare skickas till en mottagare som inte har rätt till uppgifterna*
- *Risk 2 – Listor med utställare hanteras ej enligt fastlagd process (spara i folder ”Listor” för lätt identifiering och radering).*

5.2 Syfte

Dataskyddsombudet behöver ha en kontinuerlig överblick över vilka som är de största riskerna i verksamhetens personuppgifts-behandlingar. Detta är till exempel nödvändigt för att DSO ska kunna ge rätt råd till verksamheten om vilka dataskyddsåtgärder som behöver vidtas.

5.3 Resultatet av riskkartläggningen

Risk 1 – Listor med publika besökare skickas till en mottagare som inte har rätt till uppgifterna

Den största volymen personuppgifter som Stockholmsmässan behandlar berör besökare till de arrangemang som utgör huvuddelen av verksamheten. Inom denna grupp är den största andelen besökare till publika arrangemang, det vill säga sådana som är öppna för allmänheten.

De publika besökarna är också de som är mest benägna att bli irriterade om deras personuppgifter inte hanteras korrekt – den som är i kontakt med Stockholmsmässan som privatperson är mer ”mån om” sina uppgifter än om kontakten sker i vederbörandes yrkesroll. Detta visas inte minst av att en stor majoritet av de personuppgifts-ärenden som skickas in till Stockholmsmässan kommer från privat-personer.

Samtidigt är besökarnas kontaktuppgifter intressanta för vissa av Stockholmsmässans samarbetspartners, som gärna vill kunna ta del av uppgifterna för att använda dem i sin egen marknadsföring. Stockholmsmässan har därför satt upp strikta regler och rutiner för i

vilka fall och på vilket sätt besökarnas uppgifter får föras över till samarbetspartners. Rutinerna är väl dokumenterade och de medarbetare som berörs har fått utbildning i dessa.

Det kan dock inte uteslutas att en enskild medarbetare skulle kunna begå ett misstag som innebär att en lista med besökare skickas till en samarbetspartner som inte har rätt att ta emot den, och att detta leder till irritation som i sin tur ger en ryktesskada för Stockholms-mässan.

	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

Risk 2 – Listor med utställare hanteras ej enligt fastlagd process (spara i folder ”Listor” för lätt identifiering och radering).

Under stickprovskontrollen framkom det att listor med utställare vid ett par tillfällen inte laddats upp på rätt ställe (folder ”Listor”). Detta gäller listor på utställare som tas ut ur utställarregistret för att användas till utskick. Förvaltningsgruppen har gått igenom rutinen och informationen har spridits vidare som en påminnelse för alla som hanterar listor.

Det kan dock inte uteslutas att en enskild medarbetare skulle kunna begå ett misstag som innebär att en lista inte tas bort. Den ligger dock kvar enbart internt och ingen annan har åtkomst som inte jobbar på Stockholmsmässan.

	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

Fortsätt att utbilda nya medarbetare, och att påminna befintliga medarbetare regelbundet, om hur listor med personuppgifter om besökare ska hanteras.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Stockholmsmässan planerar att genomföra stickprovskontroller på event från samtliga affärsområden under 2024.

6.2 Syfte

En av dataskyddsombudets viktigaste uppgifter är att övervaka att verksamheten lever upp till bestämmelserna i GDPR. En del i detta arbete är att göra återkommande granskningar, där DSO kontrollerar hur väl förordningstexten efterlevs och ger återkoppling till verksamheten så att rätt beslut kan tas i dataskyddsfrågor.

6.3 Planerade granskningar

Under 2024 planerar Stockholmsmässans dataskyddsombud att genomföra stickprovskontroller på samma sätt som under 2023, det vill säga att samtliga affärsområden finns representerade.

Det kommer inte att vara känt för arbetsgrupperna i förväg vilka event som ska granskas.

7 Övrigt att rapportera

7.1 Sammanfattning

Under 2023 upptogs arbetet med en förvaltningsgrupp för GDPR på Stockholmsmässan, som har i syfte att optimera och säkerställa rutiner och processer för GDPR. Förvaltningsgruppen har automatiserat vissa processer med systemstöd, och stickprovskontroller har genomförts för olika event.

7.2 Syfte

Avsikten med detta avsnitt är att ge möjlighet att komplettera bilden av statusen i dataskyddsarbetet. Här kan sådant beskrivas som inte på ett naturligt sätt tas upp under någon av punkterna i rapporteringsstrukturen ovan.

7.3 Övriga observationer

Under 2022, när verksamheten kom igång igen, genomförde man ett internt projekt för att göra ett omtag i dataskyddsarbetet. Arbetet leddes av en extern konsult med god kännedom om Stockholmsmässans verksamhet. År 2023 har rutiner och processer använts och optimerats efter verksamhetens behov så att regelefterlevnad inom GDPR sker.

Dataskyddspolicy och automatiserade processer för datahantering har uppdaterats.

7.4 DSO ger råd och rekommendationer till PUA

Inga särskilda råd eller rekommendationer.