GDPR Årsrapport

2023

SISAB

Innehåll

Bakgrund

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

Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

Skolfastigheter i Stockholm, SISAB, har 2017-2023 gjort ett omfattande arbete för att förhålla sig till Dataskyddsförordningen. Under 2023 har inget framkommit som skulle innebära ökade risker för de registrerade eller att verksamheten gjort omfattande förändringar vilka inte hanterats vad det gäller skydd för registrerade.

DSO ser inte att några allvarliga risker föreligger i dagsläget. Dock kan risker uppkomma om inte förordningen fortsätter att bibehållas.

DSO rekommenderar:

- Lämplig organisation av Informationssäkerhet/Dataskydd
- Fortsätta utbilda/informera kring behandling av personuppgifter
- Fortsätta implementera dataskydd i verksamheten

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 ledningen status och DSO slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO genomförda uppföljning och granskning.

Registerförteckning

Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	23 registreringar
Har nödvändiga uppdateringar gjorts?	Ja (DSO har rensat registret)
Bedöms registerförteckningen vara fullständig?	Inte helt, men tillräckligt för att vara godkänd.
Har verksamheten lämpliga rutiner för registerföring?	Nej, dessa ska införas med ny DSO

Syfte

Registerförteckningen ska uppdateras vid behov.

Resultat

Det finns inte någon rutin för hur registerförteckningen ska uppdateras eller revideras.
Det råder osäkerhet om alla behandlingar är registrerade.

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

DSO ger råd och rekommendationer till PUA

Registerförteckningen är en grundläggande del av dataskyddsförordningen och bör vara korrekt och uppdaterad. Rutiner för att hålla registret aktuellt bör finnas och vara implementerade i verksamheten. Om rutinerna följ bör alla behandlingar finnas registrerade

Styrdokument

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?	Delvis
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Nej

Syfte

Det ska finnas ansvar och ägandeskap av dokumentationen för dataskydd.

Resultat

Det saknas ett ansvar inom verksamheten att revidera och underhålla dokumentation kring dataskyddet. Det ansvaret måste finnas i verksamheten men kan sammanföras med ansvaret för informationssäkerheten.

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

DSO ger råd och rekommendationer till PUA

En översyn av styrdokumenten behöver genomföras och kompletteras där så behövs

Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

Sammanfattning

Fråga/kontroll	Svar
Har alla personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	Ja
Är klassade personuppgiftsbehandlingar aktuella?	Ja

Syfte

Tekniska och organisatoriska skyddsåtgärder ska vara dokumenterade

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

Konsekvensbedömningar

Sammanfattning

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

Syfte

Konsekvensbedömningar ska göras framför allt på högriskbehandlingar. Alla behandlingar ska testas för om behandlingen kan medföra en sådan risk för den registrerade att konsekvensutredning bör genomföras,

Resultat

Inga behandlingar har bedömts vara högriskbehandlingar eller av behov med konsekvensutredning.

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**

DSO ger råd och rekommendationer till PUA

I styrdokument ska framgå när konsekvensutredning ska testas

Individens rättigheter

Sammanfattning

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

Syfte

Rutin för hantering av registrerades rättigheter ska finnas på plats

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

DSO ger råd och rekommendationer till PUA

Process för hantering av registrerades rättigheter finns på plats

Personuppgiftsincidenter

Sammanfattning

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

Syfte

Process för hantering av personuppgiftsincidenter ska finnas på plats

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

Planerade granskningar under det nya verksamhetsåret

Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Registerförteckning*
- *Styrdokument*
- *PuB avtal*
- *Integritetspolicy, information kring behandlingar*
- *Incidentprocess*
- *Rutiner och instruktioner*

Rapporten är framställd av

Roger Broberg, Registrerat Dataskyddsombud för SISAB

Stockholm 2023-12-18