GDPR Årsrapport

2022

SISAB

Innehåll

Bakgrund **3**

Sammanfattning **4**

Obligatoriska rapporteringsområden **5**

Registerförteckning *6*

Styrdokument *8*

Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar *9*

Konsekvensbedömningar *10*

Individens rättigheter *11*

Personuppgiftsincidenter *12*

Genomförda granskningar under året **13**

Sammanfattning *13*

Genomförda granskningar och deras resultat *13*

Risker inom dataskydd **13**

Sammanfattning *13*

Resultatet av riskkartläggningen *14*

DSO ger råd och rekommendationer till PUA *15*

Planerade granskningar under det nya verksamhetsåret **16**

Sammanfattning *16*

Syfte *16*

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 ledningen ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att ledningen behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje ledning 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 ledning.

Denna årsrapport är således ett medel för ledningen 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 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.

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

Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

SISAB har 2017-2018 gjort ett omfattande arbete för att förhålla sig till Dataskyddsförordningen. Det arbetet har minskat i omfattning och skulle behöva revideras samt en fortsatt implementation i verksamheten.

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

DSO rekommenderar:

- Lämplig organisation av Informationssäkerhet/Dataskydd
- Under 2023 göra en fullständig genomlysning av följsamhet gentemot GDPR
- 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:ns slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda uppföljning och granskning.

Registerförteckning

Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	153 registreringar
Har nödvändiga uppdateringar gjorts?	Delvis
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Nej

Syfte

Revidering har påbörjats 2022 och beräknas vara slutförd Q1 2023

Resultat

Registerförteckningen innehåller idag både ofullständiga samt felaktiga registreringar. Registret ska revideras, kompletteras och rensas under första delen av 2023

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

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.

Styrdokument

Sammanfattning

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

Syfte

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
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	Det saknas vissa informationsklassningar
Är klassade personuppgiftsbehandlingar aktuella?	Ja

Syfte

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

Informationssäkerhetsklassning av system behöver färdigställas. Informationsklassning av processer bör utföras.

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

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

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

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

Processen bör granskas så även interna incidenter dokumenteras

Genomförda granskningar under året

Sammanfattning

- Granskning/revidering av registerförteckning har påbörjats 2022

Genomförda granskningar och deras resultat

Granskningar kommer att utföras 2023

	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

Risker inom dataskydd

Sammanfattning

Relevanta risker inom verksamheten:

- *Otillräcklig styrning av dataskydd*
- *Brister i registerförteckning*
- *Brister i informationsklassning*

Resultatet av riskkartläggningen

Risk 1

Otillräcklig styrning av dataskydd

Översyn av styrdokument avseende lämplighet, tillräcklighet och verkan

	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

Risk 2

Brister i registerförteckning

Efter färdigställd revidering/komplettering ska registret vara aktuellt. Förteckningen är viktig då den redovisar de behandlingar verksamheten genomför

	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

Risk 2

Brister i informationsklassning

Alla system där SISAB är informationsägare bör informationssäkerhetsklassas. Processer behöver informationsklassas (beröring till registerförteckning)

	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

Genom att ha en lämplig organisation på informationssäkerhet/dataskydd samt ett uttalat direktiv om att SISAB ska följa uppsatta riktlinjer och lagar ska dessa risker minimeras under året.

Planerade granskningar under det nya verksamhetsåret

Sammanfattning

Relevanta granskningsområden inom verksamheten:

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

Syfte

Under året kommer ett antal granskningar att genomföras för att påvisa brister eller förbättringar i enlighet med fastställt års-hjul.

Rapporten är framställd av

Roger Broberg, Registrerat Dataskyddsombud för Skolfastigheter i Stockholm AB

Stockholm 2022-01-06