Granskningsrapport

Mognadsundersökning av dataskydd

Vård- och omsorgsnämnden

Januari 2021

Dataskyddsombud
Lunds kommun

Security Solution Scandinavia AB
Flöjelbergsgatan 20 C
431 37 Mölndal, Sverige

Office +46 31 98 90 00
www.securitysolution.se

Innehållsförteckning

Security Solution Scandinavia AB
Flöjelbergsgatan 20 C
431 37 Mölndal, Sverige

Office +46 31 98 90 00
www.securitysolution.se

1 Bakgrund

1.1 Dataskyddsförordningen

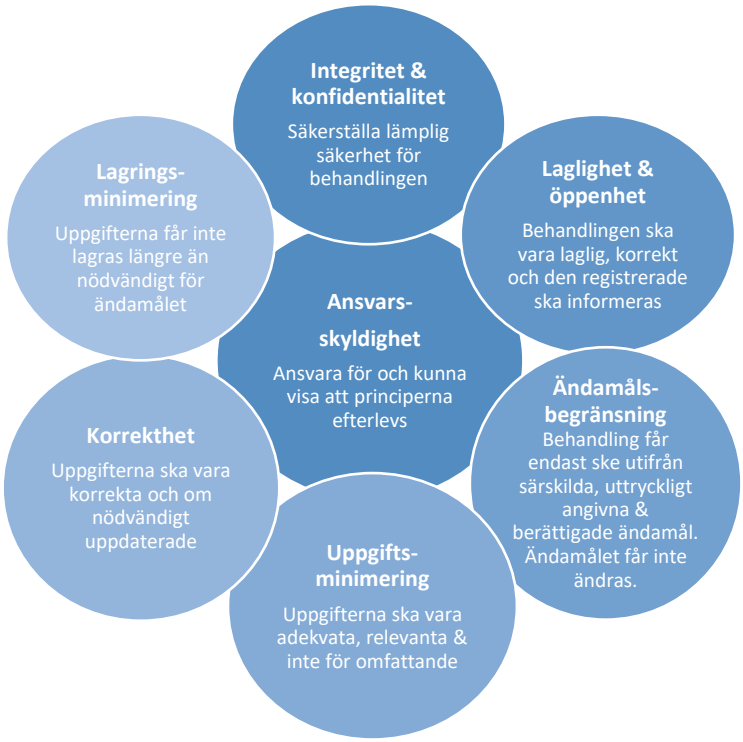
Dataskyddsförordningen (GDPR, The General Data Protection Regulation) trädde i kraft den 25 maj 2018 och gäller i hela EU. Dataskyddsförordningen har till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter så att det fria flödet av uppgifter inom Europa inte hindras. Dataskyddsförordningen har medfört skärpta skyldigheter för den som registrerar uppgifter och stärkta rättigheter för den som är registrerad i jämförelse med tidigare dataskyddslagstiftning.

2 Ansvar och roller

Personuppgiftsansvarig för den granskade verksamheten är vård- och omsorgsnämnden.

2.1 Personuppgiftsansvariges skyldigheter

Dataskyddsförordningen innehåller omfattande krav på den som behandlar personuppgifter. All behandling ska genomsyras av sex grundläggande principer som stadgas i dataskyddsförordningens Artikel 5. Den personuppgiftsansvarige ska kunna *visa på* att principerna efterlevs, detta kallas för ansvarsskyldighet. Ansvaret kan aldrig delegeras. Nedan presenteras dessa principer.



Figur 1. Illustration av personuppgiftsansvariges skyldigheter.

2.2 Dataskyddsombudets granskningsroll

Av Artikel 39 dataskyddsförordningen framgår att dataskyddsombudet ska övervaka efterlevnaden av förordningen, av andra av unionens eller medlemsstaternas dataskyddsbestämmelser och av den personuppgiftsansvariges strategi för skydd av personuppgifter. En del av detta arbete innebär att granska verksamheten i syfte att kontrollera att den efterlever förordningen.

2.3 Information om granskningen och verksamhetens omfattning

Dataskyddsombudet gav information om granskningen vid ett möte med kommunens dataskyddskontakter den 4 september 2020. Vård- och omsorgsnämnden ansvarar för vård- och omsorgsinsatser enligt socialtjänstlagen (SoL), hälso- och sjukvårdslagen (HSL), samt lagen om särskilt stöd och service till vissa funktionshindrade (LSS).

3 Syfte

Syftet med denna granskning var att med hjälp av en mognadsundersökning ge en nulägesbild över verksamhetens arbete med dataskydd, i enlighet med Dataskyddsförordningen, interna styrdokument och övrig lagstiftning.

4 Mål med mognadsundersökningen

- Ge ett nuläge som kan användas som underlag för att sedan ta fram en handlingsplan att arbeta vidare.
- Mognadsundersökningen kan användas återkommande för att spegla utveckling inom området.

5 Metod

Granskningen är en översiktlig mognadsundersökning, baserad på en validerad vetenskaplig metod utifrån en internationell mognadsskala för dataskydd (PMM)[1] som använder 73 kriterier (principer) för best practice i organisationsprocesser inom dataskydd (GAPP)[2].

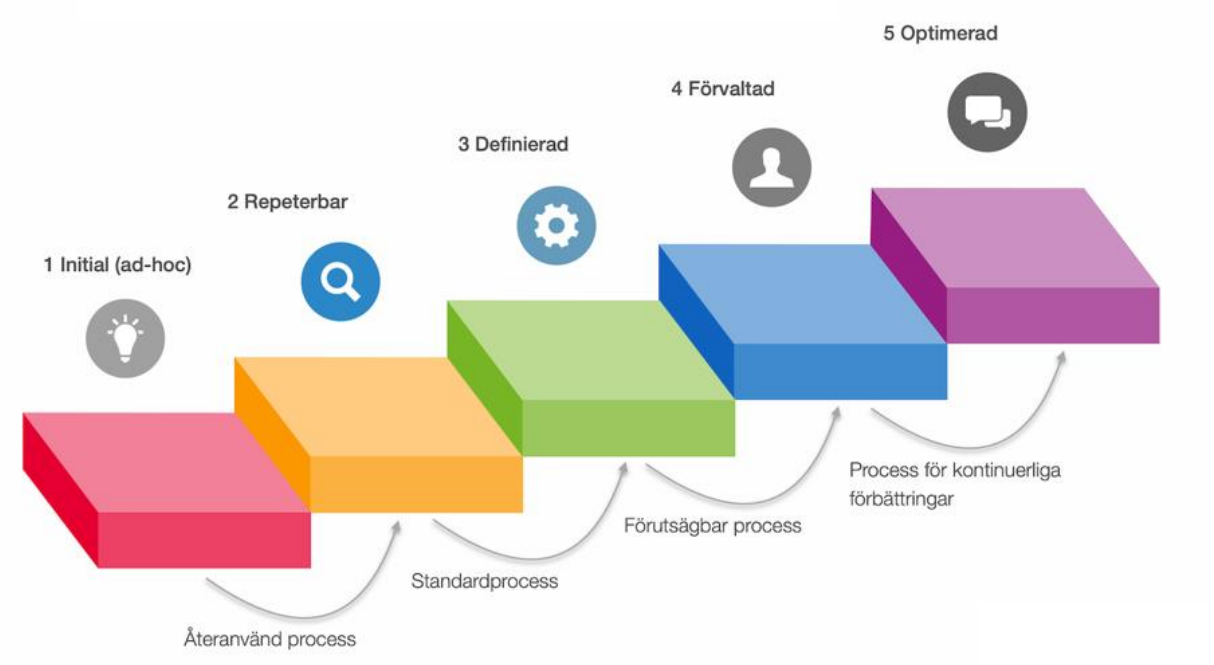
En webbenkät skickades ut till dataskyddssamordnarna i Lunds kommun den 30 november 2020. Dataskyddssamordnarna fick sedan två veckor på sig att svara på enkäten. Granskningen är en självskattning av verksamhetens mognadsnivå inom dataskydd som utgår från 23 olika kriterier anpassade för offentlig verksamhet, grupperad i sex områden:

1. Roller och ansvar
2. Styrning och efterlevnad
3. Utbildning och kompetens
4. Processer och verktyg
5. Risk och klassning
6. Incident och informationssäkerhet

[1] Privacy Maturity Model
[2] Generally Accepted Privacy Principles

Denna undersökning innehåller ett urval av de kriterier som finns med i GAPP, till exempel har samtycke, kontroll av laglig grund och inbyggt dataskydd (privacy-by-design) utelämnats. Urvalet gjordes så att enkätundersökningen kunde besvaras under en rimlig tid, och för att anpassa undersökningen för Lunds kommun.

Mognadsnivån beräknades genom att tillsätta ett värde på mellan 1 till 5 på varje kriterium, där 1 innebär en mer ad hoc hantering och 5 innebär helt optimal. Resultatet ger en god bild av mognaden för dataskydd bland nämnderna och bolagen. Rekommendationer ges baserat på var nämnden eller bolaget befinner sig i de olika områdena. Vidare ges även en benchmarking som jämförelse mot Sveriges kommuner i en undersökning från 2019, genomförd i en masteruppsats vid Göteborgs universitet[3].



Figur 2. Illustration av mognadsnivåerna.

[3] Privacy Maturity in Swedish municipalities: A Quantitative Survey Based on a Privacy Maturity Framework

6 Risker

För de olika områdena finns det risker med hanteringen som bör tas i beaktande. Riskerna är generella och är hämtade och anpassade från en nationell kartläggning och analys i utredningen *Hur står det till med den personliga integriteten? – En kartläggning av Integritetskommittén* (SOU 2016:41) samt beskrivningar i Dataskyddsförordningen. Denna rapport ger ingen värdering av riskernas sannolikhet eller konsekvenser, utan påtalar endast risker som möjliga risker, med bakgrund av de personuppgiftsbehandlingar som vård- och omsorgsnämnden utför.

6.1 Roller och ansvar

Otydliga roller och ansvarsförhållanden samt brist på kompetenta resurser kan leda till att organisationen inte arbetar systematiskt med dataskydd och informationssäkerhet, vilket innebär risker för att känsliga personuppgifter kan röjas.

6.2 Styrning och efterlevnad

Brister i styrning och kontroll av efterlevnad av dataskydd kan leda till förlust av insyn och kontroll, vilket innebär risk att känsliga personuppgifter inte hanteras rätt i kommunikation inom och mellan olika myndigheter eller andra organisationer.

6.3 Utbildning och kompetens

Brist på intern utbildning och kompetens kan leda till generella risker och brister i beställarkompetens, avseende tillämpning av dataskydd och informationssäkerhet, juridik och kravställning.

6.4 Processer och verktyg

Bristande processer och verktyg innebär att ansvarstagande för hur uppgifter hanteras inte följer dokumentationskrav och att tillmötesgå registrerades rättigheter, vilket får följden att den enskilde har litet inflytande över myndighetshanteringen.

Det finns även risk att personuppgifter hanteras utan att korrekta juridiska biträdesavtal är tecknade, vilket leder till att personuppgifter kan hanteras för biträdets egna ändamål.

6.5 Risk och klassning

Brister i hantering av risker och klassning av personuppgifter kan leda till att man inte identifierar vilken information man har och vilka möjliga risker som finns för individerna. Bedömning av sannolikheten för att riskerna inträffar och allvarligheten om de inträffar riskerar därför att inte göras korrekt, vilket leder till att man inte kan säkerställa *lämpliga* tekniska eller organisatoriska åtgärder gällande integritet och konfidentialitet.

6.6 Incident och informationssäkerhet

Brister i processer och rutiner för att säkerställa att säkerhetsincidenter (och eventuella personuppgiftsincidenter) hanteras korrekt (genom snabb och effektiv identifiering, samt kontroll och undersökning av incidenter), kan leda till att överträdelser och intrång inte upptäcks, vilket innebär risker för att personuppgifter kan röjas, förvanskas eller bli otillgängliga.

7 Resultatet från mognadsundersökningen

I detta avsnitt presenteras resultatet från enkätundersökningen. Tabellen nedan visar mognadsvärdet per kriterium sorterat efter områdena. Det är upp till personuppgiftsansvarig att bestämma vilken nivå verksamheten ska sträva efter.

Vård- och omsorgsnämnden	Mognadsvärde
Roller och ansvar	
1.1.2 Definierade roller och ansvar	3
1.2.8 Tillgängliga resurser finns	3
10.2.5 Övervakning av hur effektiva kontrollerna är	1
Styrning och efterlevnad	
1.1.0 Integritetspolicy	3
1.2.2 Regelverket i linje med lagstiftningen	3
1.2.5 Intern granskning av avtal	2
10.2.3 Efterlevnadskontroll	2
10.2.4 Rapportering av avvikelser	2
Utbildning och kompetens	
1.2.9 Kvalifikationer på intern personal	2
1.2.10 Utbildning och medvetenhet av dataskydd	4
Processer och verktyg	
7.2.2 Hantering av leverantörer och PUB-avtal	3
5.2.2 Lagring av personuppgifter (dokumenthantering)	4
6.2.3 Verifiering av individers identitet	5
6.2.1 Registrerades rättigheter (registerutdrag)	4
2.2.1 Information om personuppgiftshantering	3
Risk och klassning	
1.2.4 Riskhantering	3
1.2.6 Konsekvensbedömningar	2
1.2.3 Informationsklassning	2
Incidenthantering och informationssäkerhet	
8.2.1 Informationssäkerhet (funktion och hantering)	3
1.2.7 Incidenthantering	3
8.2.6 Skydd för mobila enheter	2
8.2.2 Logisk skydd (intrångdetektering, granskning av loggar etc..)	1
8.2.7 Test av effektiviteten av säkerhetsåtgärder	1
Mognadsmedelvärde	**2,65**

8 Rekommendationer

De rekommendationer som ges är baserat på resultatet från denna enkätundersökning. De indikerar det som behöver göras för att uppnå nästa steg i mognadstrappan, se figur 2.

8.1 Roller och ansvar

- Ledningen bör vara ansvarig för att övervaka processen att tilldela roller och ansvar för att kontrollera att det utförs korrekt, att kommunikationen fungerar, samt att nödvändig information och material finns tillgängligt. Se även till att ansvarig för dataskyddsfrågor är en del av ledningsgruppen och att denne person har en god kunskapsnivå inom området dataskydd.
- Ledningen bör säkerställa att nödvändiga resurser identifieras och görs tillgängliga genomgående för att stödja olika arbeten som inkluderar skydd av personuppgifter.
- Se över hur effektiva kontrollerna är som har till syfte att utvärdera verksamhetens regelefterlevnad av dataskyddsförordningen.

8.2 Styrning och efterlevnad

- Inför efterlevnadskontroller av regelverket och använd resultatet av kontrollerna för att förstärka arbetet med dataskydd.
- Se till att processen för att genomföra återkommande jämförelser även inkluderar en kontinuerlig bevakning av ny lagstiftning på dataskyddsområdet.
- Se till att upprätta avtal med samtliga leverantörer, avtalen ska innehålla reglering av personuppgifter (t.ex. personuppgiftsbiträdesavtal), och se till att samtliga avtal granskas.
- Dokumentera processen för efterlevnadskontroll och se till att den täcker alla aspekter för efterlevnad av regler, lagar samt andra externa och interna krav.
- Dokumentera processer och rutiner som inkluderar alla relevanta aspekter för att hantera avvikelser och korrigeringar. Se även till att alla avvikelser är fullt dokumenterade.

8.3 Utbildning och kompetens

- Definiera de kvalifikationer som ska innehas av den personal som behandlar personuppgifter. Se till att de personer som är ansvariga för säkerheten och skyddet av personuppgifter har fått lämplig utbildning.
- Se till att utbildningsprogrammet är obligatorisk för den personal som berörs. När det förekommer incidenter bör förnyad och framtagen utbildning och informationskampanjer genomföras.

8.4 Processer och verktyg

- Inför rutin för att övervaka förändringar på tredje partens tekniska miljö för att säkerställa att de fortsatt lever upp till kravställningarna
- Granska regelbundet efterlevnaden av dokumenthanteringsplanen, och se till att förändringar eller avvikelser övervakas och processen uppdateras som en följd av detta.
- Inför en automatiserad process för sökning och sammanställning av registerutdrag med själv-service i ett tekniskt system, och genomför regelbunden uppföljning av processen.
- Se till att den registrerade meddelas om dess personuppgifter avser användas för ett annat ändamål, så snart det är praktiskt möjligt. Inför också en process för spårning av versioner av meddelanden och kommunikation kring informationen i syfte att veta vilken information som givits, vid varje givet tillfälle exempelvis versionshantering.

8.5 Risk och klassning

- Som en följd av riskbedömningarna bör regelverk och processer uppdateras i syfte att förbättra dem och göra dem mer effektiva. Till exempel går det att använda ett verktyg (som t ex ett IT-stöd) för hantering och dokumentation av risker. Det bör även genomföras interna och externa revisioner som inkluderar risker kopplat till personuppgifter.
- Inför en formell process för hur konsekvensbedömningar ska genomföras som täcker införande och förändringar i produkter, tjänster, verksamhet och infrastruktur.
- Se till att alla behandlingar är klassade och har riskbedömts.

8.6 Incidenthantering och informationssäkerhet

- Ledningen bör övervaka och följa upp sårbarheter och avvikelser, till exempel genom regelbundna granskningar av arbetet med mätetal som kan jämföras över tid och med andra (benchmark).
- Genomför tester av incidenthanteringsprocessen genom övningar som även inkluderar ledningen, och genomför övervakning med hjälp av tekniska kontroller för att identifiera incidenter.
- Skapa en rutin och process för skydd av mobila enheter och se till att granska efterlevnaden, samt genomför tester av säkerheten.
- Inför grundläggande säkerhetsfunktioner för inloggning och behörigheter.
- Genomför regelbundna tester av olika säkerhetsfunktioner.

9 Jämförelse med riksmedelvärde 2019

I tabellen nedan visas en jämförelse med vård- och omsorgsnämndens resultat och riksmedelvärdet för 2019 fördelat på de sex områdena. Detta visar hur nämnden ligger i förhållande i riket generellt. Dock bör det påpekas att undersökningsresultat jämförs med 2019 år nationella resultat, vilket kan innebära att det finns visst utrymme för skillnader mot innevarande år på nationell nivå.

Områden	**Vård- och omsorgsnämnden**	**Riksmedelvärde**
Roller och ansvar	2,33	1,99
Styrning och efterlevnad	2,40	1,92
Utbildning och kompetens	3,00	1,80
Processer och verktyg	3,40	2,38
Risk och klassning	2,33	1,94
Incidenthantering och informationssäkerhet	2,00	1,88
Medelvärde	**2,65**	**2,01**

10 Avslutningsvis

Vård- och omsorgsnämndens dataskyddsarbete ligger på en övergripande mognadsnivå på 2,65 vilket innebär att processer och rutiner generellt finns och är implementerade men att det finns en del förbättringsområden, bland annat vad gäller övervakning av efterlevnadskontroller, logiskt skydd, och testning av säkerhetsåtgärder. Vård- och omsorgsnämnden har kommit längre i sitt dataskyddsarbete vad gäller utbildning och medvetenhet, dokumenthanteringsplan, verifiering av individers identitet vid registerutdrag, och registrerades rättigheter.

Dataskyddsombudet har kännedom om att vård- och omsorgsnämnden har hanterat två personuppgiftsincidenter under perioden 2020-09-01 – 2020-12-21.

Denna undersökning är en självuppskattning vilket innebär att resultatet påverkas av den verksamhetskännedom och kunskap inom ämnesområdena som den/de som besvarade enkäten har. Eftersom svaren resulterar i ett uppskattat mognadsvärde ger det ändå en värdefull nulägesbild av var verksamheten befinner sig i sitt dataskyddsarbete. Denna undersökning kan även bidra till att öka förståelsen och mognaden hos personuppgiftsansvarig, och med stöd från rekommendationerna kan en handlingsplan skapas för kommande års arbete med dataskydd.

Ett sätt att se hur vård- och omsorgsnämndens dataskydd utvecklas är att återkommande svara på denna enkät, eller liknande mognadsundersökningar.