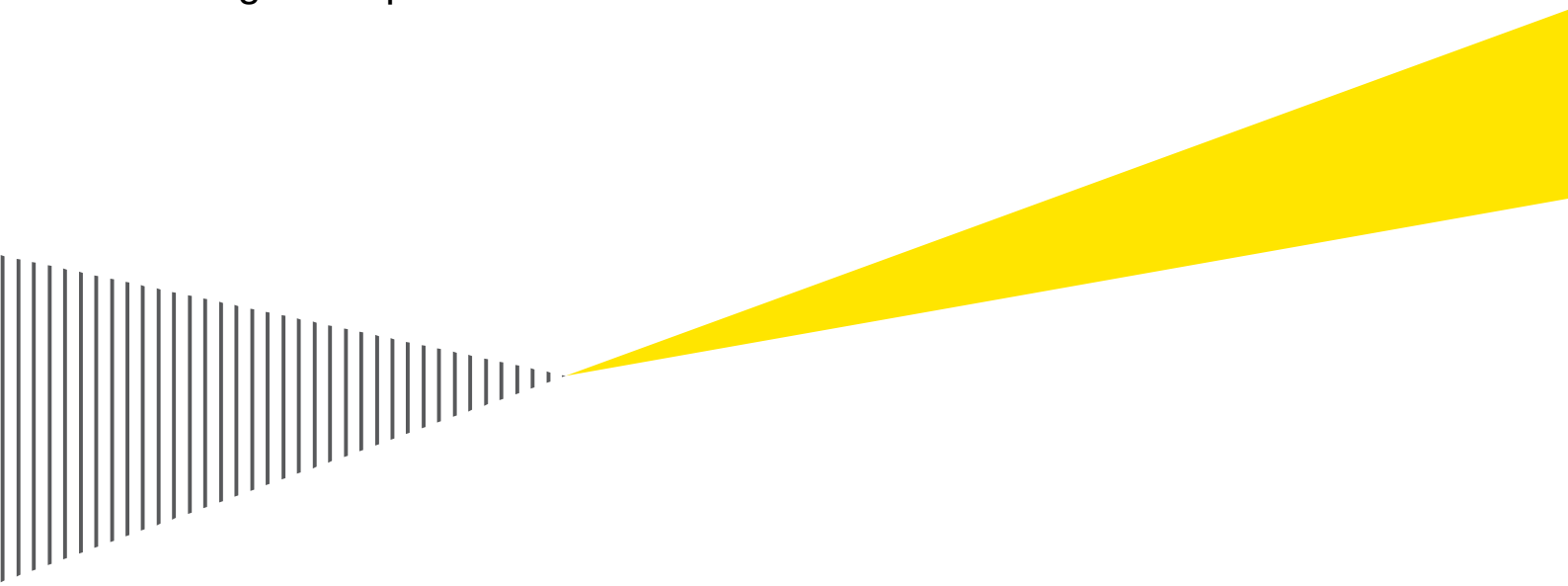
Revisionsrapport nr 4/2019

Upplands Väsby kommun

Granskning av kommunens arbete med dataskyddsförordningen

Augusti-september 2019



Building a better working world

Sammanfattande bedömning

EY har på uppdrag av Upplands Väsby kommuns förtroendevalda revisorer genomfört en granskning i syfte att undersöka hur kommunen arbetar med dataskyddsförordningen och hur kommunens mognad ser ut avseende de åtgärder som förordningen stipulerar.

I granskningen används EY:s metod för granskning av mognad gentemot dataskyddsförordningen. Enligt metoden bedöms kommunens mognadsnivå i 116 frågor/krav på en ordinarie skala från 1 (*ej på plats*) till 5 (*aktiv*). Kraven är kategoriserade över flera områden.

För Upplands Väsby kommun ligger många av kraven på nivå **4 (*implementeras*) eller 5 (*aktiv*)**. Detta betyder att majoriteten av processerna och rutinerna har dokumenterats och är för närvarande på gång att förankras och kommuniceras, eller att dessa redan är aktiva utan väsentliga brister. Genomsnittet över alla krav ligger på närmare fyra beaktandes att mycket är på gång att implementeras.

Nedan visas fördelning för alla kontrollpunkter. För att kunna besluta om vilka åtgärder som bör prioriteras bör organisationen beakta risker kopplat till brister inom varje enskild kontroll. Som princip bör allt som inte är ”aktivt” adresseras.

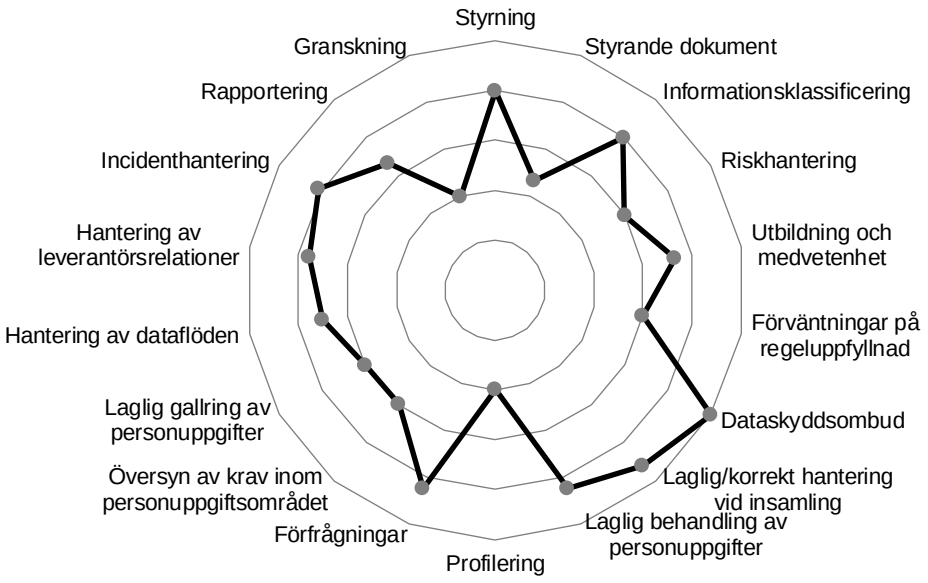
		1	2	3	4	5	
	Ej tillämpligt	Ej på plats	Diskuteras	Planeras	Implement-eras	Aktiv	Ø
Krav per mognads-nivå	8	16	9	8	26	49	3,77

Resultat och mognadsnivåer inom respektive område sammanfattas på sida 3. Brister – delvis väsentliga - har identifierats inom flera områden. Genomsnittet per område indikerar vilka områden som har störst förbättringsbehov, men på grund av genomsnittsberäkningen kan t.ex. ett område med grön färgkod ändå sakna viktiga kontroller. Respektive krav har inte viktats i genomsnittsberäkningen, och granskningens huvudsakliga värde ligger förslagsvis i dess observationer och rekommendationer som beskrivs i en bredare kontext i själva granskningsrapporten (se sida 11).

Överlag hamnar snittet uppåt fyra, dock har några observationer av grundläggande allvarligare karaktär noterats. Kommunstyrelsen rekommenderas åtgärda dessa skyndsamt:

- Det saknas en person som ansvarar för att åtgärda de befintliga och delvis identifierade gapen i kommunens arbete med dataskyddsförordningen.
- Det saknas en uppdaterad informationssäkerhetspolicy och uppdaterade riktlinjer för informationssäkerhet som är utformade enligt dataskyddsförordningens krav och som kan vara utgångspunkt till formella interna granskningar av styrande dokument för integritetsskydd.
- Det saknas en rutin som säkerställer att internutbildningar om dataskyddsförordningen uppdateras över tid och sker vid nyanställning.
- Det saknas rutiner och/eller kontroller som säkerställer att personuppgifter endast behandlas för de ändamål som de samlades in för.
- Det saknas en rutin för att uppdatera instruktioner och styrande dokument enligt nya krav inom personuppgiftsområdet.
- Kommunen genomför inga regelbundna tester som kontrollerar att befintliga rutiner och legala krav gällande laglig gallring av personuppgifter efterlevs.

Område	Krav per nivå						Genomsnitt ø
		1	2	3	4	5	
	Ej tillämpligt	Ej på plats	Diskuteras	Planeras	Implementeras	Aktiv	
Styrning			1		2	2	**4,0**
Styrande dokument		1	1		1		**2,3**
Informationsklassificering		1				3	**4,0**
Riskhantering		5		1	2	4	**3,0**
Utbildning och medvetenhet		1				2	**3,7**
Förväntningar på regeluppfyllnad			1	1	1		**3,0**
Dataskyddsombud						5	**5,0**
Laglig/korrekt hantering vid insamling		1				9	**4,6**
Laglig behandling av personuppgifter		1	1		3	8	**4,2**
Profilering	1		1				**2,0**
Förfrågningar	1	1			3	5	**4,2**
Översyn av krav inom personuppgiftsområdet		1				1	**3,0**
Laglig gallring av personuppgifter	1	1	2	1	2	1	**3,0**
Hantering av dataflöden		1			2	1	**3,0**
Hantering av leverantörsrelationer	5	1		1	5	2	**3,8**
Incidenthantering			2	1	4	6	**4,1**
Rapportering				2	1		**3,3**
Granskning		1		1			**2,0**
	8	**16**	**9**	**8**	**26**	**49**	**3,8**



Nedan sammanfattas alla observationer per granskat område.

Område	Observationer
Styrning	1. Det saknas en person som ansvarar för att åtgärda de befintliga och delvis identifierade gapen i kommunens arbete med dataskyddsförordningen. 2. Det saknas regelbundna kommunikationsinsatser som informerar om kommunens dataskyddsmål för befintliga anställda och vid nyanställning. 3. Det saknas central analys och koordinering i arbetet med övriga lagar som påverkar behandlingen av personuppgifter.
Styrande dokument	4. Det saknas en uppdaterad informationssäkerhetspolicy och uppdaterade riktlinjer för informationssäkerhet som är utformade enligt dataskyddsförordningens krav och som kan vara utgångspunkt till formella interna granskningar av styrande dokument för integritetsskydd.
Informations-klassificering	5. Informationsklassificeringar görs inte för ostrukturerad information.
Riskhantering	6. Riskanalyser uppdateras inte vid återkommande intervaller. 7. Det saknas metod och ansvar för att genomföra konsekvensbedömningar innan verksamheten startar en ny typ av behandling.
Utbildning och medvetenhet	8. Det saknas en rutin som säkerställer att internutbildningar om dataskyddsförordningen uppdateras över tid och sker vid nyanställning.
Förväntningar på regeluppfyllnad	9. Roller och ansvar kopplat till arbetet med dataskydd är inte tydliga. 10. Kunskapen om Datainspektionens befogenheter, uppgifter och förväntningar är inte formellt dokumenterat eller kommunicerat och uppdateras inte i en regelbunden systematisk process. 11. Enskilda behandlingar av personuppgifter är inte dokumenterade i Draftit.
Laglig/korrekt hantering vid insamling	12. Det saknas en process för hur kommunen kommunicerar möjliga förändringar i hur man hanterar personuppgifter.
Laglig behandling av person-uppgifter	13. Ändamålen och den rättsliga grunden till behandlingen är inte dokumenterade för alla behandlingar av personuppgifter. 14. Det saknas rutiner och/eller kontroller som säkerställer att personuppgifter endast behandlas för de ändamål som de samlades in för.
Profilering	15. Det är idag inte säkerställt att verksamhetens beslut som endast är grundade på automatiserad behandling sker i enlighet med de tillåtna undantagen i artikel 22.
Förfrågningar	16. Det finns ingen rutin för att avgöra om den registrerades begäran anses vara ogrundad. 17. Det saknas möjlighet att enkelt kunna sammanställa och extrahera data i ett maskinläsbart format. 18. Det är inte säkerställt att system uppfyller kravet att kunna markera personuppgifter som begränsade och otillgängliga.
Översyn av krav inom personupp-giftsområdet	19. Det saknas en rutin för att uppdatera instruktioner och styrande dokument enligt nya krav inom personuppgiftsområdet.

Laglig gallring av personuppgifter	20. De befintliga gallringsrutinerna följer en årlig cykel och utgår inte från det faktiska borttagsbehovet under året. 21. Det saknas IT-stöd med funktionalitet som automatiskt markerar personuppgifter för borttagning. 22. Kommunen genomför inga regelbundna tester som kontrollerar att befintliga rutiner och legala krav gällande laglig gallring av personuppgifter efterlevs.
Hantering av dataflöden	23. Ingen periodisk genomgång för behörigheter med åtkomst till personuppgifter görs. 24. Verksamheten har inte dokumenterat dataflöden avseende hur personuppgifter rör sig mellan verksamhetens IT-system.
Hantering av leverantörs-relationer	25. Personuppgiftsbiträdesavtal finns inte till alla externa leverantörer. 26. Det saknas en egen rutin som regelbundet säkerställer att personuppgiftsbiträden agerar på ett sätt som innebär att dataskyddsförordningen efterlevs över tid, varken i upphandlingsfasen eller senare. 27. Det saknas en arbetsmetod som säkerställer att personuppgiftsbiträdesavtal uppdateras vid legala eller interna förändringar.
Incidenthantering	28. Information till registrerade som drabbas av personuppgiftsincidenter ingår inte i processkartan för incidenthantering. 29. Hittills har kommunen inte etablerat utvärderingar på hur väl de interna incident-instruktionerna efterlevs.
Rapportering	30. Det saknas en formell rutin för mer frekventa/ad-hoc rapporter till styrelse/nämnd och krav som sådan rapportering ska utgå ifrån. 31. Det saknas en formell rutin för att svara på förfrågningar från Datainspektionen.
Granskning	32. Kommunen har ingen fastslagen granskningsplan eller internkontrollfunktion med fokus på dataskyddsarbetet och dataskyddsförordningens krav.

Innehållsförteckning

1. Inledning

1.1. Bakgrund

Den 25e maj 2018 trädde dataskyddsförordningen, även känd som GDPR efter engelskans General Data Protection Regulation, i kraft till fullo. Dataskyddsförordningen gäller i alla EU:s medlemsländer och ersatte i Sverige den äldre personuppgiftslagen (PUL) från 1998. Syftet med dataskyddsförordningen är att stärka enskilda personers skydd av personuppgifter, underlätta det fria flödet av personuppgifter på den digitala marknaden samt minska den administrativa bördan. I jämförelse med exempelvis PUL har dataskyddsförordningen även kommit med skärpta sanktioner i händelse av fall där förordningens artiklar inte uppfylls. De obligatoriska kraven för dataskyddsförordningen inkluderar:

- Både offentliga och privata institutioner skall kunna beläggas med sanktioner utefter samma bedömningskriterier (upp till 10 till 20 MSEK för offentliga verksamheter beroende på överträdelsens allvarlighetsgrad)
- Obligatorisk överträdelseanmälan rörande personuppgiftsincidenter skall göras till den lokala tillsynsmyndigheten inom 72 timmar efter att incidenter har uppdagats. Lokal tillsynsmyndighet i Sverige är Datainspektionen (DI)
- Individer har rätt till ersättning i form av skadestånd till följd av överträdelser av förordningen av en personuppgiftsansvarig eller ett personuppgiftsbiträde

Med bakgrund i ovan genomförde EY på uppdrag av Upplands Väsby kommuns förtroendevalda revisorer under juni 2019 en granskning av hur kommunen arbetar för att uppnå dataskyddsförordningens direktiv.

1.2. Syfte

Syftet med granskningen var att ge en övergripande nulägesbild av huruvida Upplands Väsby kommun bedriver ett ändamålsenligt arbete med dataskyddsförordningen och hur kommunens mognad ser ut i uppfyllelse av de åtgärder som förordningen stipulerar.

1.3. Avgränsningar

De observationer som presenteras i denna rapport baseras enbart på den information som inhämtats under intervjuer och genom inspektion av erhållen dokumentation, såsom styrdokument, riktlinjer och planer (se sektion 3). Granskningen är begränsad till arbetet som Upplands Väsby kommun bedriver på kommuncentral nivå och inga av kommunens nämnder, förvaltningar eller kommunalägda bolag har således granskats ytterligare. Ingen teknisk analys har genomförts och inga stickprov på efterlevnad har tagits.

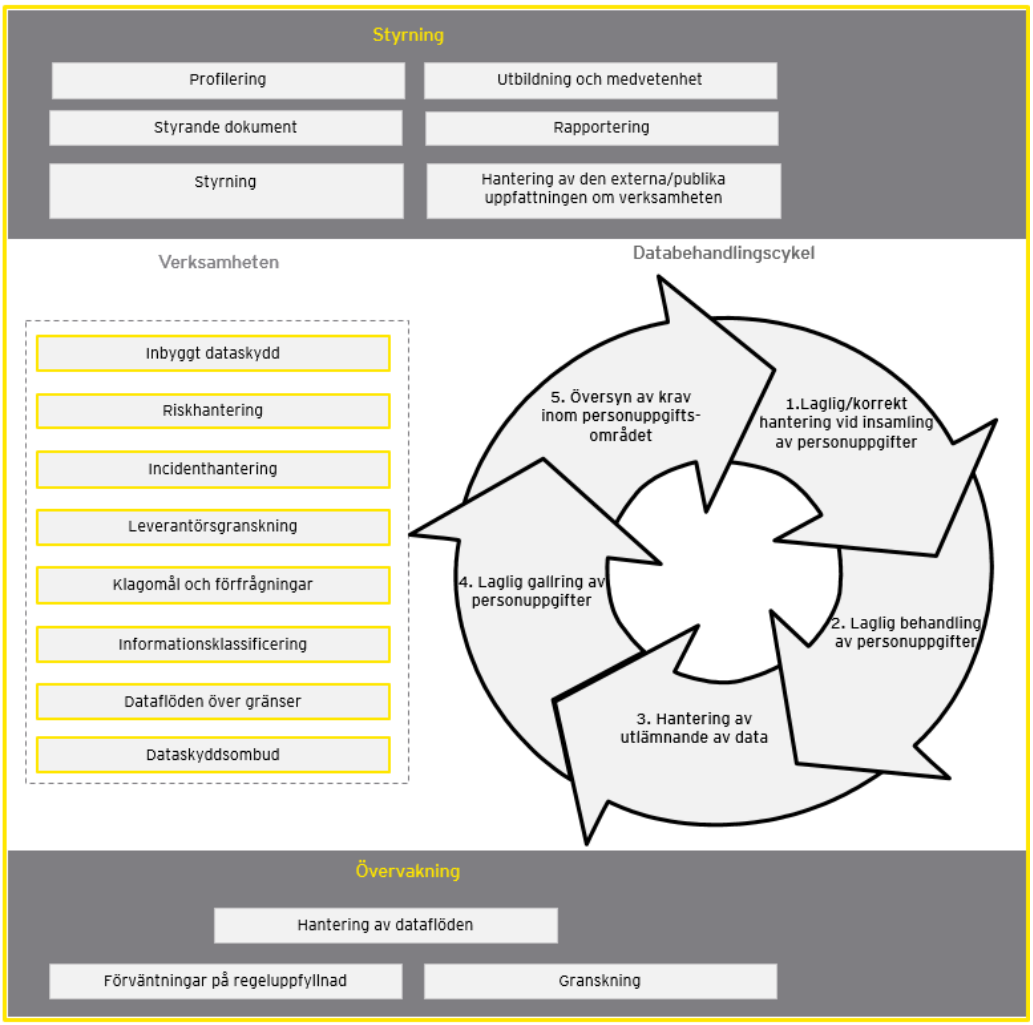
1.4. Metod och genomförande

Granskningens syfte har adresserats genom intervjuer med identifierade nyckelpersoner i kommunens arbete med dataskyddsförordningen samt genomgång av relevant dokumentation (se Sektion 3. Bilaga: Källförteckning). Granskningen är utförd mot god praxis och med utgångspunkt i EY:s metod för granskning av mognad gentemot dataskyddsförordningen.

Metoden består av ett ramverk med 116 frågor. Dessa frågor är kategoriserade över 22 områden kopplade till dataskyddsförordningen. Frågorna är både direkt kopplade till krav från förordningen och indirekt kopplade genom att täcka exempelvis styrning och underhåll av arbetet med att upprätthålla regeluppfyllnaden. För enkelhetens skull används ordet ”krav” synonymt i rapporten oavsett om det avser en direkt eller indirekt koppling. Metoden understryker premissen att det är viktigt att inte bara titta på huruvida enskilda kontroller är på plats och enskilda krav är täckta, det är även av stor vikt att säkerställa att styrning och

uppföljning av regeluppfyllnad sker systematiskt.

Bilden nedan visar de områden som innefattas av ramverket.[1]



[1] I slutrapporten täcks områdena ”Hantering av den externa/publika omfattningen om verksamheten” och ”Inbyggt dataskydd” av de övriga områdena. Områdena ”Hantering av utlämnande av data” och ”Klagomål och förväntningar” förenas i området ”Förfrågningar”. Områdena ”Leverantörsgranskning” och ”Dataflöden över gränsen” förenas i området ”Hantering av leverantörsrelationer”.

Utifrån graden av mognad inom respektive krav erhåller områdena en färgkod för att kunna visa en översiktlig helhetsbild av Upplands Väsby kommuns mognad i arbetet med dataskyddsförordningen.

	Mognadsnivå	Definition	Bristnivå
	0 Ej tillämpligt	Frågan ej tillämplig för Upplands Väsby kommun	Ej tillämpligt
	1 Ej på plats	Processen, rutinen, funktionen eller motsvarande existerar ej	Väsentliga brister
	2 Diskuteras	Diskussioner pågår kring hur man ska formalisera och förankra processen, rutinen, funktionen eller motsvarande	Väsentliga brister
	3 Planeras	Det finns utkast på processer, rutiner eller motsvarande men de är inte formellt förankrade i verksamheten än	Bristfällig
	4 Implementeras	Processer, rutiner eller motsvarande har dokumenterats och håller för närvarande på att förankras och kommuniceras	Bristfällig
	5 Aktiv	Processer, rutiner, funktioner eller motsvarande är aktiva UTAN VÄSENTLIGA BRISTER	Inga väsentliga brister

Ett områdes färgkod visar en genomsnittlig mognadsnivå som beräknas över alla krav som ingår i området. Respektive krav har inte viktats. Ett område med grön färgkod är att anse som bristfällig och kan t.ex. sakna kritiska, obligatoriska processer samtidigt som det kan innehålla processer som är aktiva utan väsentliga brister.

Ett område ska därför till exempel endast anses som aktivt om alla dess krav ligger på nivå 5, endast anses som bristfälligt utan väsentliga brister om all dess krav ligger minst på nivå 3, och så vidare.

Varje områdes genomsnittliga mognadsnivå kompletteras i rapporten med en beskrivande sammanställning över hur kommunens mognad bedöms.

Exempel: Område ”Styrelse” med fem krav

Ø 4,0

Implementeras

1 | 2 | 2

← Kommunens genomsnittlig mognad i arbetet med områdets krav:

Mognadsnivå	Krav per mognadsnivå	Viktat	
2	1	2	
4	2	8	
5	2	10	
	5	**20**	20 ÷ 5 = **4,0**

← Antal krav per mognadsnivå i området

Granskningens huvudsakliga värde ligger i dess observationer och rekommendationer som beskrivs i en bredare kontext i själva granskningsrapporten.

1.5. Faktagranskning

De intervjuade nyckelpersonerna har beretts tillfälle att faktagranska rapporten och lämna

synpunkter på dess innehåll.

2. Observationer och rekommendationer per område

2.1. Styrning och styrande dokument

2.1.1. Styrning

Styrning *syftar till att undersöka verksamhetens dataskydds- och integritetsrelaterade mål samt verksamhetens strategi för att uppnå målen. Detta område täcker också hur målen har definierats, kommunicerats och hur ofta de granskas.*

Upplands Väsbys dataskydds- och integritetsrelaterade mål och strategi syftar till att det ska vara säkerställt att kommunen följer EU:s dataskyddsförordning och att det ska finnas en väl bearbetad struktur samt processer och ansvar för hur kommunen hanterar behandlingar av personuppgifter.

Mot denna bakgrund har kommunen genomfört ett *Projekt för anpassning till nya dataskyddsförordningen (GDPR)* för att utvärdera om det finns områden inom förordningen där man inte uppfyller dess krav. I detta syfte har projektet genomfört workshops med samtliga kontor för att ta fram övergripande processer, förslag på organisation, roller och utbildningsprogram och för att identifiera behandlingar av personuppgifter och kontaktpunkter där kommunen samlar in personuppgifter. Projektet resulterade 2017 i en slutrapport samt gapanalys och åtgärdsplan och var tänkt som utgångspunkt till kommunens framtida styrningsarbete i dataskyddsfrågor. I dagsläget saknas dock en person som ansvarar för att man åtgärdar de identifierade gapen. Planen att inkludera åtgärdspunkterna i ett projekt *Ledningssystem för informationssäkerhet (LIS)* följs inte med anledning av att digitaliseringsdirektören och övrig personal som har varit involverat i arbetet med dataskyddsförordningen har lämnat kommunen.

Verksamheten har gjort tydligt för dem som hanterar personuppgifter för verksamhetens räkning vad följderna kan bli om dataskyddsförordningen inte efterlevs och på det sättet kommunicerat sina mål i hanteringen av personuppgifter: Relevant information om mål och möjliga konsekvenser ingick i utbildningar som genomfördes under april 2018 i flera steg. Detta inkluderades även i ytterligare informationssessioner som kommunens dataskyddsombud höll för olika grupper och kontor innan förordningens införande. Dessa utbildningsinsatser har man dock inte upprepat sedan dess, vilket medför att nyanställda inte är informerade om målen och möjliga konsekvenser. Som konsekvens ökar risken att man inte efterlever regelverket.

Kommunen har i övrigt inte centralt analyserat vilka andra lagar än den europeiska dataskyddförordningen som kan påverka behandlingen av personuppgifter och därmed inte centralt tydliggjort effekter av detta – varken i styrdokument eller utbildningar. Detta ansvar ligger därför mycket på nämnderna, kontoren och deras GDPR-representanter.

Observationer

Det saknas en person som ansvarar för att åtgärda de befintliga och delvis identifierade gapen. Det saknas regelbundna kommunikationsinsatser som informerar om dataskyddsmål för befintliga anställda och vid nyanställning. Det saknas centralt analys och koordinering i arbetet med övriga lagar som påverkar behandlingen av personuppgifter.

Rekommendationer

1. Sätt ett tydligt ansvar och tidsplan för att åtgärda de identifierade gapen och driva dataskyddsarbetet framöver. (HÖG PRIO)
2. Genomför regelbundna kommunikations- eller utbildningsinsatser kopplat till kommunens dataskydds- och integritetsrelaterade mål.

ø 4,0
Implementeras
1 | 2 | 2

3. Analysera centralt vilka andra lagar som påverkar behandlingen av personuppgifter och tydliggör deras effekter på behandlingen.

2.1.2. Styrande dokument

Styrande dokument *syftar till att bedöma om verksamheten har utformat en integritetspolicy eller motsvarande styrande dokument, som ställer krav på att processer (eller motsvarande) och kontroller införs för att skydda verksamhetens personuppgifter. Detta handlar om formell utveckling, dokumentation, granskning och godkännande av verksamhetens styrande dokument för integritetsskydd.*

Kommunen har utformat en informationssäkerhetspolicy som kommunfullmäktige har antagit i november 2016. Den beslutade policyn och dess kompletterande riktlinjer är inte längre giltiga sedan december 2017 och har inte varit utformad för att täcka kraven i dataskyddsförordningen. Integritetsskydd ingår till exempel inte som ett eget mål i policyn. Sedan november 2016 har kommunfullmäktige inte sett över eller reviderat styrdokumenten.

En remissversion av policyn med datum november 2018 finns men har inte blivit antagen av kommunfullmäktige än. Arbetet på en remissversion av informationssäkerhetsriktlinjer är påbörjat men inte slutfört. Därmed saknar kommunen ett beslutat regelverk, beträffande hantering av personuppgifter, som är uppdaterat enligt dataskyddförordningens krav. Nämnderna har inte tagit fram egna policyer för att kompensera gapen.

Dataskyddsombudet har, i linje med sin uppgift att övervaka efterlevnaden av dataskyddsförordningen, i början av 2019 lämnat sin årliga rapport om aktiviteter och händelser från det förgående året. Inom ramen för detta har det kommunicerats rekommendationer. Behovet av en uppdaterad informationssäkerhetspolicy och riktlinje för informationssäkerhet lyfts i rapporten. I och med att policyn inte är på plats har dataskyddsombudet dock inte haft möjlighet att granska om organisationen följer interna styrdokument.

Observationer

Det saknas en uppdaterad informationssäkerhetspolicy och uppdaterade riktlinjer för informationssäkerhet som är utformade i linje med dataskyddsförordningens krav, och som kan vara utgångspunkt till formella interna granskningar av styrande dokument för integritetsskydd.

Rekommendationer

1. Besluta och implementera ett regelverk beträffande hantering av personuppgifter som är uppdaterade i enlighet med kraven i dataskyddsförordningen.
2. Sätt upp rutiner för att följa upp att styrdokumenten efterlevs.

ø 2,3
Diskuteras
1 1 1

2.2. Informationsklassificering och riskhantering

2.2.1. Informationsklassificering

Informationsklassificering *ska vara baserad på känsligheten hos personuppgifter och användas för att välja ut och implementera lämpliga skyddsåtgärder för att skydda den information som hanteras. Valet av skyddsåtgärder ska bestämmas beroende på den inverkan det skulle ha på de registrerade om deras personuppgifter skulle förloras, bli stulna, olämpligt offentliggöras, ändras eller förstöras.*

Upplands Väsby kommun använde 2017 och 2018 SKL:s verktyg KLASSA för att klassificera information som finns i sökbar form (*strukturerad information*). Klassificeringar i KLASSA görs explicit utifrån kraven i dataskyddförordningen och kriterier som riktighet, konfidentialitet och tillgänglighet. Utöver det används en egen webbaserad applikation, Draftit Privacy, som register över alla sparade typer av personuppgifter. Detta täcker även hur uppgifterna behandlas av kommunen och i vilka system behandlingar sker. I klassificeringsprocessen tar man hänsyn till möjliga konsekvenser som skulle kunna inträda om personuppgifter skulle förloras, bli stulna, olämpligt offentliggöras, ändras eller förstöras. I detta sammanhang skiljer kommunens klassificering mellan vad som menas med känsliga personuppgifter och övriga personuppgifter. Begreppens definition enligt dataskyddsförordningen återfinns i Draftit och har kompletterats med tillägg från Dataskyddsinspektionen. Dataskyddsombudet har kommunicerat begreppens betydelse under sina informationssessioner i 2018.

Informationsklassificeringar görs dock inte för information som inte finns i sökbar form (*ostrukturerad information*, t.ex. löpande text).

Observationer	ø **4,0**
Informationsklassificeringar görs inte för ostrukturerad information.	Implementeras
Rekommendationer	1 3
1. Klassificera ostrukturerad information/data.	

2.2.2. Riskhantering

Riskhantering *syftar till att utvärdera hur verksamheten identifierar och minskar integritetsrisker i sin verksamhet och i sina IT-komponenter. Detta inkluderar att bedöma vilka skyddsåtgärder (t.ex. anonymisering, kryptering) som är viktiga för att mildra integritetsrisken inom verksamheten.*
Detta handlar specifikt om att analysera var/hur aktiviteterna kan tänkas orsaka risker gentemot individers fri- och rättigheter, och att analysen sker så tidigt som möjligt i aktiviteter (projekt, förändringar, ...) för att säkerställa att skyddet av integritet är inbyggt från början (som standard) i dessa aktiviteter.
Inbyggt dataskydd undersöker i detta sammanhang huruvida verksamheten har processer eller rutiner på plats som säkerställer att man genomför en konsekvensanalys avseende integritetshantering/personuppgifter i början av (eller under) projekt och verksamhetsförändringar.

Personuppgifter klassificeras i KLASSA genom att man sätter skadenivåer på kriterierna riktighet, konfidentialitet och tillgänglighet. Nivåerna beskriver möjliga konsekvenser som kan bli aktuella när information inte är tillförlitlig, korrekt och fullständig, när åtkomst till den begränsas eller när den inte kan nyttjas i förväntad utsträckning samt av rätt person. Kriteriet konfidentialitet tar hänsyn till tänkbara konsekvenser för enskilda individers integritet. Kommunens verktyg för informationsklassificeringar bidrar därmed till riskidentifieringen och har även resulterat i en handlingsplan som har kommunicerats ut till alla kontor för att mildra integritetsrisker. Ansvaret att hantera risker ligger på systemansvariga som har som uppgift att anpassa skyddsåtgärder utifrån riskanalyserna. Systemansvariga finns till alla system.

Dataskyddsförordningens perspektiv utgår främst från den registrerads rättigheter. I KLASSA:s aggregerade riskbedömningar konkurrerar den registrerads rättigheter dock med verksamhetens behov av åtkomst till tillförlitlig information. Det finns en fördel i att identifiera och bedöma integritetsrisker som en egen riskkategori innan dessa ingår i en kombinerad riskanalys. Detta kan göras för att visa att man hanterar personuppgifter som en särskild informationsklass vilkens skydd väger tyngre än verksamhetens behov. I Draftit Privacy finns idag en sådan möjlighet att sätta risknivåer per personuppgiftsbehandling - utifrån uppgifternas och behandlingens typ. Metoden används dock inte av kommunen.

Informationsklassificeringen i 2017/18 och dokumentationen i Draftit Privacy skedde mest med anledning av dataskyddsförordningens omedelbara införande och siktade på att registerföra befintliga behandlingar av personuppgifter. Förordningens krav gäller utöver det för alla nya behandlingar: Innan en ny typ av behandling startas ska kommunen genomföra en konsekvensbedömning som använder en metod för att identifiera och minska risker som annars kan leda till att individers integritet äventyras.

Idag saknas dock riktlinjer eller ansvar som säkerställer att kommunen gör konsekvensbedömningar och att man söker råd från Datainspektionen i de fallen där bedömningar visar höga risker ur integritetssynpunkten.

Det saknas utöver det rutiner och ansvar som säkerställer att informationsklassificeringar och övriga riskanalyser (t.ex. i Draftit Privacy) uppdateras regelbunden.

Observationer

Riskanalyser uppdateras inte vid återkommande intervaller och det saknas metod och ansvar för att genomföra konsekvensbedömningar innan verksamheten startar en ny typ av behandling.

Rekommendationer

1. Implementera en rutin för att uppdatera informationsklassificeringar och övriga riskanalyser vid återkommande intervaller för att säkerställa att inga nya eller förändrade risker har uppstått. Sätt tydliga ansvar för rutinen.
2. Implementera en metod för att genomföra konsekvensbedömningar innan verksamheten startar en ny typ av behandling. Metoden ska definiera när och hur verksamheten ska samråda med myndigheten. Sätt tydliga ansvar.

ø 3,0

Planeras

5 | | 1 | 2 | 4

2.3. Organisation och ansvar

2.3.1. Utbildning och medvetenhet

Utbildning och medvetenhet *är viktiga komponenter för implementeringen av dataskyddsförordningen för att säkerställa medvetenheten hos anställda inom en verksamhet. Det finns även en del nyckelroller som är nödvändiga för att förankra integritetsfrågor genom hela verksamheten: t.ex. dataskyddsombud med större kunskap inom ämnet.*

Upplands Väsby kommun har 2018 genomfört ett GDPR introduktionsprogram med alla anställda. En del av introduktionsprogrammet bestod av en strukturerad utbildning i form av en webkurs som bygger på en serie 2 till 3 minuters ämnesspecifika lektioner som skickades ut direkt till medarbetarna via e-post. Kursen tillhandahölls av leverantören Junglemap som är specialiserad i utbildningar kring informationssäkerhet och dataskydd. Leverantörens utbildningsplattform NanoLearning erbjuder ett uppföljningsverktyg vilket användes av kommunen för att säkerställa att anställda slutförde utbildningen. Den andra delen av introduktionsprogrammet bestod av informationssessioner och frågestunder i klassrumsformat som hölls av kommunens dataskyddsombud i samarbete med kontoren.

Kommunen har inte kört liknande utbildningsinsatser vid nyanställning eller etablerat en process som säkerställer att internutbildningar om dataskyddsförordningen uppdateras och genomförs regelbundet även för befintliga anställda. Kommunen har sagt upp avtalet med Junglemap. Därmed erbjuder kommunen inte längre någon möjlighet att delta i strukturerade utbildningar som anställda frivilligt kan delta i. Utbildningen är begränsad till en sektion med vanliga frågor och svar kring dataskyddsförordningen som finns på intranätet.

Observationer

Det saknas en rutin som säkerställer att internutbildningar inom dataskyddsförordningen uppdateras över tid och sker vid nyanställning.

Rekommendationer

1. Implementera en rutin som säkerställer regelbundna, uppdaterade utbildningar och säkerställ att alla anställda slutför utbildningen. (HÖG PRIO)

Ø 3,7

Planeras

1 | | | | 2

2.3.2. Förväntningar på regeluppfyllnad

*Tillsynsmyndighetens **förväntningar på regeluppfyllnad** innebär att verksamheter är skyldiga att förstå de integritetslagar och krav som är aktuella i de jurisdiktioner som de är verksamma i. Verksamheter är också skyldiga att förstå vad som förväntas av dem från Datainspektionen, och deras tillhörande uppgifter och befogenheter. Verksamhetens olika delar bör kunna kartlägga de krav som finns i de jurisdiktioner man är verksam i. Vidare bör verksamheten skapa förutsättningar för god rapportering i de dagliga verksamhetsprocesserna (eller motsvarande).*

Kommunen har etablerat en egen dataskyddsfunktion med mål att bygga särskild kunskap om dataskyddsförordningens krav och för att möta Datainspektionens förväntningar. Funktionen består av en informationssäkerhetssamordnare, av ett dataskyddsombud och av en GDPR-representant från respektive kontor. Dataskyddsfunktionen och dess aktörer upplever sina roller och ansvar delvis som otydliga på grund av att det saknas en beslutad informationssäkerhetspolicy med ansvarsfördelning, särskilt efter den tidigare informationssäkerhetssamordnaren har lämnat kommunen vid årsskiftet 2018/19.

Dataskyddsfunktionen håller regelbundna möten där man diskuterar befintliga och uppdaterade lagliga krav, deras tolkning och verksamhetens övriga aktuella dataskyddsfrågor. Dataskyddsombudet är dataskyddsfunktionens länk till tillsynsmyndigheten och har tagit del av två av Datainspektionens informationsdagar, vilket har bidragit till en bättre förståelse av myndighetens förväntningar på regeluppfyllnad. Kommunens kunskap om myndighetens befogenheter, uppgifter och förväntningar är dock inte formellt dokumenterad vilket ökar personberoendet i organisationen. Utöver deltagandet på informationsdagarna finns dessutom inget strukturerat sätt för att periodvist fånga upp ändringar i DI:s roll och krav.

Dokumentationen som återfinns i Draftit Privacy bidrar till att Upplands Väsby kommun kan motivera för tillsynsmyndigheten att behandlingsgrunder finns där kommunen behandlar (känsliga) personuppgifter. Dokumentationen saknas dock i dagsläget för enstaka behandlingar av personuppgifter och arbetet att komplettera dokumentationen pågår.

Observationer

Roller och ansvar kopplat till arbetet med dataskydd är inte tydliga. Kunskapen om DI:s befogenheter, uppgifter och förväntningar är inte formellt dokumenterat eller kommunicerat och uppdateras inte i en regelbunden, systematisk process. Enskilda behandlingar av personuppgifter är inte dokumenterade i Draftit.

Rekommendationer

1. Besluta en informationssäkerhetspolicy eller övriga styrdokument som sätter tydliga roller och ansvar till dataskyddsfunktionen. (HÖG PRIO)
2. Dokumentera den befintliga kunskapen om DI:s roll och krav och uppdatera dokumentationen systematiskt och regelbundet.
3. Komplettera dokumentationen i Draftit Privacy för de behandlingar av personuppgifter där den saknas idag.

Ø 3,0

Planeras

	1	1	1	

2.3.3. Dataskyddsombud

Dataskyddsombud *berör dataskyddsombudet för verksamheten samt dess kompetens, förutsättningar och stöd för att kunna utöva sin roll på ett tillfredsställande sätt.*

Varje nämnd har utsett Upplands Väsbys kommunjurist till sitt dataskyddsombud. I och med att dataskyddsombudet har en bakgrund som jurist finns goda förutsättningar för att personen uppfyller förordningens krav om sakkunskap om lagen, och har förmåga att övervaka regelverkets efterlevnad. Dataskyddsombudets goda förutsättningar har stärkts genom en dedikerad utbildning i dataskyddsförordningens innehåll samt dataskyddsombudens roll i organisationen. I sitt dagliga arbete utnyttjar dataskyddsombudet dessutom sitt eget nätverk för informations- och kunskapsutbyte, där också SKL ingår, för att säkra kompetensen.

Dataskyddsombudet agerar på ett självständigt sätt med ledningens förtroende och med en etablerad rapporteringsväg till kontorscheferna. Han upplever att hans arbete stöds med tillräckligt många resurser, både i form av personal och IT-verktyg som Draftit Privacy, för att kunna uppfylla sina arbetsuppgifter utan att intressekonflikter uppstår. Denna bedömningen utgår dock ifrån den nuvarande arbetsbelastningen och stödet till dataskyddsombudet bör utökas i fall att hans ansvar utökas med ytterligare ramverk, rutiner och granskningar.

Observationer

Rekommendationer

1. Utvärdera granskningens observationer och rekommendationer och deras konsekvenser för dataskyddsombudets roll framöver. Säkra tillräckligt stöd.

Ø 5,0
Aktiv
5

2.4. Behandling av personuppgifter

2.4.1. Laglig/korrekt hantering vid insamling av personuppgifter

Vid den tidpunkt då personuppgifter samlas in måste verksamheten ge den registrerade information om syftet med insamlingen, hur personuppgifterna ska användas, huruvida personuppgifterna kommer att delas med tredje part, överföras utanför EU/EES etc. Denna information ska finnas i ett sekretessbelagt meddelande.

Projektet för anpassning till nya dataskyddsförordningen (GDPR) har identifierat insamlingspunkter för personuppgifter (blanketter och kommunens e-tjänst) och tagit fram informationstexter som godkändes av kommunjuristen. Efter projektets avslutning har nämnderna ansvarat för att inkludera informationstexterna vid insamlingspunkterna. Man har utformat texterna med tanke på att de ska innehålla information om syftet med insamlingen, om hur de insamlade personuppgifterna kommer användas och sparas, om hur personuppgifter delas med tredje part, om den registrerades rättigheter (information, rättning, överföring, begränsning, borttag) och om kontaktmöjligheter till dataskyddsombudet och Datainspektionen.

Det finns idag ingen process för hur verksamheten kommunicerar med de registrerade kring hur verksamhetens hantering av personuppgifter hos verksamheten kommer förändras framöver, om sådana förändringar planeras. Anledningen till detta är att de personuppgifter som behandlas av kommunen anses som väldigt statiska med låg risk att sådana förändringar kommer att ske.

Blanketternas utformade och kravet på e-legitimation i e-tjänsten förutsätter att individernas samtycke bygger på en aktiv handling och är distinkt, tydligt och inte ihopblandat med andra samtycken: Olika samtycken samlas in för olika användningsområden. Samtycken sparas.

Kommunen har genomfört vissa åtgärder i sina system för att leva upp till kraven på inbyggt dataskydd i insamlingen, exempelvis har man försökt minimera fritextrutor för att begränsa användarnas möjligheter att fylla i eller ta del av information som inte efterfrågas i kommunens godkända personuppgiftsbehandlingar.

Observationer

Det saknas en process för hur kommunen kommunicerar möjliga förändringar i hur man hanterar personuppgifter.

Rekommendationer

1. Implementera en rutin för hur verksamheten ska kommunicera med de registrerade kring hur man hanterar personuppgifter framöver, om förändringar i hanteringen av personuppgifter planeras.

Ø 4,6

Implementeras

1 | | | | 9

2.4.2. Laglig behandling av personuppgifter

Laglig behandling av personuppgifter *kräver att en verksamhet ska specificera ändamålen för insamlandet när den samlar in personuppgifter. Verksamheten måste säkerställa att den använder den personliga informationen enbart för de tidigare specificerade ändamålen. Om de vill använda personuppgifterna för ytterligare ändamål så måste de utvärdera om det är förenligt att göra så.*

Upplands Väsby Kommun har implementerat Draftit Privacy som ett elektroniskt register över personuppgiftsbehandlingar. Registret är utformat enligt dataskyddsförordningens krav, särskilt enligt kraven som sätts i artikel 30. Ansvaret att registret förs enligt kraven och att all obligatorisk information återfinns i applikationen ligger på varje personuppgiftsansvarig.

Arbetet med att dokumentera behandlingar i registret pågår sedan 2018 och idag finns det ungefär 650 dokumenterade behandlingar i Draftit. Dokumentationen omfattar insamlingens ändamål och rättsliga grund. Det finns dock enskilda behandlingar som inte är dokumenterade eller där dokumentationen inte är fullständig. Därmed uppfyller man i enskilda fall inte kravet att verksamheten ska kunna visa att behandlingen är nödvändig för att följa en lagstadgad skyldighet eller att en behandling motiveras genom allmänt intresse eller samtycke. Registret är en stor del av kommunens dataskyddsarbete och uppdateras och kompletteras löpande.

Det finns inte rutiner/kontroller på plats för att över tid säkerställa att personuppgifter endast behandlas för det eller de ändamål som de ursprungligen samlades in för. Här ligger ansvaret på den gemene anställd som har tillgång till personuppgifterna i systemen. Om en anställd håller sig till det ursprungliga och dokumenterade ändamålet beror mest på om han eller hon informerar sig om de ändamålen som listas i Draftit Privacy. Kommunens systemansvariga har satt upp behörighetsstrukturen så att åtkomst till personuppgifter begränsas till anställda som behöver uppgifterna i sitt dagliga arbete och som är medvetna om behandlingsgrunder.

Observationer

Ändamålet och den rättsliga grunden till behandlingen är inte dokumenterade till alla behandlingar av personuppgifter. Det saknas rutiner och/eller kontroller som säkerställer att personuppgifter endast behandlas för de ändamål som de

Ø 4,2

Implementeras

samlades in för.

1 1 3 8

Rekommendationer

1. Komplettera dokumentationen i Draftit Privacy med ändamål och rättslig grund till alla behandlingar av personuppgifter.
2. Implementera rutiner och/eller kontroller för att säkerställa att utvärderingar sker innan befintliga personuppgifter används för ytterligare ändamål.

2.4.3. Profilering

Profilering *syftar till att undersöka om verksamhetens rutiner för profilering lever upp till lagkraven. Det handlar även om medvetenhet hos anställda inom verksamheten angående automatiserade behandlingar.*

Verksamheten är till en viss del medveten om huvudregeln i lagen som kräver att beslut om registrerade som i betydande grad påverkar denna inte enbart får grundas på automatiserade behandlingar om inget av dataskyddsförordningens undantag enligt artikel 22 är applicerbart. Regleringar som gäller profilering har inte varit ett fokusområde i dataskyddsombudets arbete med anledning att kommunen och dess nämnder inte använder mycket automatiserade beslutsmekanismer. Det finns dock medvetenhet om att profilering bör vara ett fokusområde framöver, särskilt med tanke på att utsträckningen av automatiserade beslut förväntas bli större när kommunens digitaliseringsinsatser fortskrider.

Observationer

Det är idag inte säkerställt att verksamhetens beslut som endast är grundade på automatiserad behandling sker i enlighet med de tillåtna undantagen i artikel 22.

Rekommendationer

1. Utöka kunskapen om de nya och mer strikta reglerna kring rätten att inte bli föremål för beslut som enbart grundas på automatiserad behandling och implementera rutiner som säkerställer att de lagliga kraven efterlevs.

ø 2,0

Diskuteras

1

2.4.4. Förfrågningar

Förfrågningar *analyserar i vilken omfattning förfrågningar kring integritet hanteras effektivt inom verksamheten. Verksamheten måste ha en process för att hantera förfrågningar som görs rörande enskildas rättigheter och bör ha rutiner för att hantera utlämnande av personuppgifter för att säkerställa att det görs enligt dataskyddsförordningens krav*

Vid insamlingen av personuppgifter och i övrigt kommunicerar Upplands Väsby kommun och dess nämnder att dataskyddsombudet är kommunens och nämndernas huvudsakliga kontaktperson i integritetsfrågor. I övrigt finns det GDPR-representanter till varje nämnd som stödjer dataskyddsombudet och som också har kunskapen för att kunna eskalera och hantera förfrågningar som inte riktas direkt till dataskyddsombudet.

Det finns kontroller som säkerställer att den registrerades identitet bevisas i samband med att personuppgifter begärs ut: Antingen skickar den registrerade sin förfråga via kommunens e-tjänst med krav på e-legitimation eller identifierar sig personligen på kommunens kontor. Utskicket av personuppgifter sker sedan endast till den registrerades folkbokföringsadress.

Kommunen har dokumenterade arbets-steg för att hantera förfrågningar och har som mål att senast inom en månad kunna besvara en förfråga.

I ett första arbets-steg tar en representant på kommunledningskontoret emot förfrågan och registrerar den i ett ärendehanteringssystem. Här saknas det formella rutiner för att avgöra om en begäran är ogrundad. Därför hanteras förfrågningar enligt den registrerades begäran. I ett andra steg informerar kommunkontorets representant alla GDPR representanter inom berörda kontor som sedan koordinerar hanteringen internt. För att uppnå målet att besvara förfrågningar inom en månad har kommunen och nämnderna kartlagt personuppgifter till system och ansvariga. Detta stöts av dokumentationen i Draftit Privacy.
I slutet av processen sammanställs all insamlad information under kommunkontorets ledning. Om förfrågan begär ett registerutdrag så skickar man sammanställningen vidare till den registrerade i ett läsbart format. Här saknas för nuvarande en möjlighet att extrahera all information i ett maskinläsbart format som till exempel kan transfereras till en tredje part på den registrerades begäran. Om förfrågan begär att kommunen ska korrigera eller radera personuppgifter beslutar man om ändringen innan den genomförs och kommuniceras. Rätten att bli bortglömt anses delvis vara begränsad i en kommun i de fallen där personuppgifter är nödvändiga för att kunna fullgöra kommunens myndighetsutövning.

För nuvarande är det inte säkerställt att kommunens system uppfyller kraven att kunna markera personuppgifter som begränsade och otillgängliga medan kommunen behandlar förfrågningar. Ansvaret att inte behandla uppgifter som ingår i en löpande granskning ligger därför på de anställda. Medvetandenivån om detta är begränsad. Systemansvariga är dock inblandade i förfrågningsprocessen och medvetna om eventuella begränsningar.

Observationer

Det finns ingen rutin för att avgöra om den registrerads begäran anses vara ogrundad. Det saknas möjlighet att enkelt kunna sammanställa och extrahera data i ett maskinläsbart format. Det är inte säkerställt att system uppfyller kravet att kunna markera personuppgifter som begränsade och otillgängliga.

Rekommendationer

1. Implementera en rutin för att bedöma om en förfråga är ogrundad eller inte.
2. Implementera maskinläsbara sammanställningar av personuppgifter.
3. Säkerställ att personuppgifter markeras som begränsade och otillgängliga medan en förfrågning behandlas.

ø 4,2

Implementeras

1 | | | 3 | 5

2.4.5. Översyn av krav inom personuppgiftsområdet

Översyn av krav inom personuppgiftsområdet *utforskar huruvida verksamheten håller sig uppdaterad med ändringar i regler och lagar inom området. Om regler/lagar ändras på ett sådant sätt att verksamhetens hantering av personuppgifter måste ändras behöver verksamheten analysera hur detta påverkar de existerande processerna, rutinerna, policyerna och riktlinjer osv.*

Dataskyddsombudet håller sig uppdaterad med ändringar i regler och lagar, även i sin funktion som kommunjurist, och ansvarar för att ge råd till de personuppgiftsansvariga, så att de är informerade om kommunens skyldigheter i dataskyddsfrågor. För att hålla sig uppdaterad i sektorspecifika lagar avseende personuppgifter använder dataskyddsombudet sig av information från SKL som bevakar och analyserar ändringar i lagstiftningen på uppdrag av sina medlemmar. Utöver detta deltar dataskyddsombudet i DI:s GDPR forum.

I dagsläget saknas dock en etablerad rutin för att uppdatera kommunens instruktioner eller motsvarande styrande dokument över tid så att dessa hålls anpassade till ändringar som sker i lagstiftning. Ett övergripande ledningssystemet där dataskydd ingår är ännu inte på plats, och dataskyddsombudet saknar insyn om nämnder har tagit fram egna lokala riktlinjer. Bristen är tydlig med tanke på att det saknas en beslutad informationssäkerhetspolicy som är utformad enligt dataskyddsförordningens krav.

Observationer

Det saknas en rutin för att uppdatera instruktioner och styrande dokument enligt nya krav inom personuppgiftsområdet.

Rekommendationer

1. Skapa en rutin för att uppdatera framtagna instruktioner eller motsvarande styrdokument över tid så att dessa hålls anpassade till ändringar som sker i lagstiftning eller i övriga riktlinjer.

Ø 3,0
Planeras
1				1

2.4.6. Laglig gallring av personuppgifter

Personuppgifter får inte sparas längre än nödvändigt, vilket innebär att verksamheten måste ha utvecklat lämpliga policys och rutiner (eller motsvarande beroende på verksamhet) för dokumenthantering och datalagring för att förhindra att detta sker.

Kommunen har tillsatt en kommunarkivarie och en arkivredogörare till varje kontor som har som uppgift att säkerställa laglig gallring av personuppgifter. I arbetsuppgifterna ingår att arkivredogöraren ska upprätthålla och aktualisera handlingsanvisningar för gallring av personuppgifter. Handlingsanvisningar sparas i kommunens intranät med möjlighet att filtrera efter nämnd eller verksamhet och system. De innehåller information om hur länge personuppgifter ska bevaras och förvaltas. Arkivredogörarna följer de uppsatta instruktionerna i en manuell process där man raderar eller anonymiserar personuppgifter. Processen sker årligen och därför sker gallringen enligt en fastställd tidsperiod och inte omedelbart när uppgifterna inte längre behövs för det syfte de samlades in för eller ner samtycket löper ut. Det saknas IT-stöd för att automatiskt kunna radera personuppgifter eller för att kunna markera uppgifter för borttagning vid lagringsperiodens angivna slut.

Dataskyddsfunktionen har som ansvar att genomföra regelbundna tester, undersökningar och utvärderingar för att garantera att personuppgifter inte sparas längre än nödvändigt. Ansvaret uppfylls i dagsläget inte och dataskyddsfunktionen diskuterar hur regelbundna granskningar kan täckas in i kommunens arbete med internkontroll.

Observationer

De befintliga gallringsrutinerna följer en årlig cykel och utgår inte från det faktiska borttagsbehovet under året. Det saknas IT-stöd med funktionalitet som automatiskt markerar personuppgifter för borttagning. Kommunen genomför inga regelbundna tester som kontrollerar att befintliga rutiner och lagliga krav gällande laglig gallring av personuppgifter efterlevs.

Rekommendationer

1. Implementera rutiner för att radera eller anonymisera personuppgifter när dessa inte längre är nödvändiga för det syftet de samlades in för.
2. Implementera IT-system med funktionalitet som automatiskt markerar personuppgifter vid lagringsperiodens angivna slut.
3. Genomför regelbundna tester för att garantera laglig gallring av uppgifter.

Ø 3,0
Planeras
1	2	1	2	1

2.4.7. Hantering av dataflöden

Hantering av dataflöden *fokuserar på de processer och rutiner som är associerade med att hantera hela livscykeln för personuppgifter. Detta inkluderar hantering av personuppgifter. Det handlar även om att skapa arbetsflöden för att kunna skapa och modifiera användarkonton, samt granska och rapportera personuppgifter.*

Upplands Väsby kommun fokuserar på att begränsa åtkomsten till sparade personuppgifter via en ändamålsenlig struktur för användarbehörigheter och ändamålsenliga tilldelnings- och borttagningsprocesser för behörigheter. Behörigheter styrs via single-sign-on i katalogtjänsten Active Directory där IT-avdelningen tilldelar behörigheter i en definierad beställningsprocess som kräver ett godkännande från den anställdes närmaste chef. Beställningar och godkännanden dokumenteras i kommunens e-tjänst. En anställdes konto i Active Directory stängs automatiskt vid dess avslutningsdatum om det ligger i systemet.

För nuvarande genomför systemansvariga eller chefer dock inga periodiska genomgångar av behörigheter för att säkerställa att behörigheter har tagits bort eller anpassats för de anställda som har bytt avdelning eller lämnat kommunen. Systemförvaltarna driver ett projekt med mål att sätta en gemensam struktur för behörighetshantering som ska säkerställa att kontroller finns på plats för att kunna täcka de bakomliggande riskerna.

Verksamheten har hittills inte dokumenterat dataflöden avseende hur personuppgifter rör sig mellan IT-system. Detta försvårar hanteringen av dataflöden och implicerar att behörigheter idag inte är fullständigt utformade utifrån dataskyddsförordningens perspektiv (för att explicit begränsa åtkomst till personuppgifter till de som behöver tillgång för att utföra legitimerade personuppgiftsbehandlingar eller granskningar, t.ex. i sammanhang med förfrågningar).

Observationer

Ingen periodisk genomgång för behörigheter med åtkomst till personuppgifter görs. Verksamheten har inte dokumenterat dataflöden avseende hur personuppgifter rör sig mellan verksamhetens IT-system.

Rekommendationer

1. Säkerställ att generella IT-kontroller finns för att effektivt täcka de vanliga riskerna kring behörighetshanteringen.
2. Dokumentera dataflöden avseende hur personuppgifter rör sig mellan IT-system och använda behörigheter för att segregera flödet och begränsa åtkomst till personuppgifter.

Ø 3,50

Planeras

1 | | | 2 | 1

2.5. Hantering av leverantörsrelationer

Vid kontrakt och förpliktelser med tredjeparts-leverantörer måste sekretesskrav övervägas för att skydda personuppgifter. ***Hantering av leverantörsrelationer*** *krävs för att kontrollera att de processer eller rutiner som finns på plats är lämpliga för att säkerställa att skyddet av personuppgifter följs.*

I applikationen Draftit Privacy har kommunen inventerat alla de IT-system och tjänster som behandlar personuppgifter och som tillhandahålls till leverantörer. Dokumentationen i Draftit Privacy beskriver även vilka personuppgifter som är tillgängliga eller tillhandahålls till en

leverantör. Därmed har man skapat en viktig förutsättning för att kunna uppfylla sitt ansvar som personuppgiftsansvarig. Samtidigt med inventeringen har kommunen börjat sitt arbete med att komplettera kontrakt med personuppgiftsbiträdesavtal. Detta för att fastställa rättigheter och skyldigheter enligt dataskyddsförordningens krav, t.ex. kravet att leverantörer måste rapportera personuppgiftsincidenter till Upplands Väsby kommun.

Arbetet har resulterat i ca 100 avtal som täcker majoriteten av kommunens leverantörer, och det pågår fortfarande. Kommunen har använt SKL:s mall för personuppgiftsbiträdesavtal och SKL:s checklista vid upprättandet av personbiträdesavtalen för att kvalitetssäkra att avtalsmallen innehåller relevanta avtalspunkter och GDPR-krav.

Nämndernas GDPR-representanter har huvudansvaret att regelbundet säkerställa att personuppgiftsbiträden agerar på ett sätt som innebär att dataskyddsförordningen efterlevs över tid. I Draftit Privacy finns en enkel möjlighet att skicka frågor om efterlevnad direkt till leverantörer och på så sätt att göra uppföljningar, men det saknas en egen rutin som till exempel utnyttjar just den funktionen. Granskningar av leverantörer ingår istället i internkontrollens befintliga rutiner för avtalsuppföljningar som genomförs stickprovsbaserat.

Man förlitar sig i stor utsträckning på att personuppgiftsbiträdesavtalen säkerställer och kontroller att leverantörerna uppfyller sina förpliktelser. Detta förtroende i leverantörernas agerande finns redan i upphandlingsfasen där man inte granskar att leverantören uppfyller kraven och där man istället förlitar sig på ett skriftligt godkännande från leverantören.

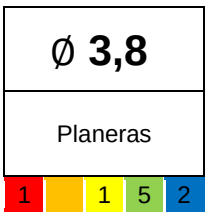
Det finns dessutom ingen arbetsmetod för att säkerställa att relevanta krav och klausuler i personuppgiftsbiträdesavtal uppdateras vid behov baserat på förändringar i regelverk eller interna förväntningar.

Observationer

Personuppgiftsbiträdesavtal finns inte till alla externa leverantörer. Det saknas en egen rutin som regelbundet säkerställer att personuppgiftsbiträden långsiktigt agerar i linje med dataskyddsförordningen, varken i upphandlingsfasen eller senare. Det saknas en arbetsmetod som säkerställer att personuppgiftsbiträdesavtal uppdateras vid lagliga eller interna förändringar.

Rekommendationer

1. Fortsätt arbetet med att ingå personuppgiftsbiträdesavtal med externa leverantörer.
2. Implementera en rutin som regelbundet säkerställer att personuppgiftsbiträden agerar enligt personuppgiftsbiträdesavtal och GDPR:s krav, både vid upphandling och senare. Granskningar kan till exempel ske utifrån SKL:s checklista som kommunen har använt vid avtalens upprättande.
3. Implementera en rutin för att säkerställa att personuppgiftsbiträdesavtal är uppdaterade i enlighet med förändrade lagliga och interna förutsättningar.



2.6. Incidenthantering

Incidenthantering *syftar till att bedöma hur verksamheten hanterar en personuppgiftsincident genom en tydligt definierad process eller rutin för att identifiera, rapportera, bedöma, avhjälpa och där så är lämpligt rapportera integritetsincidenter. En process eller rutin bör vara på plats för att undersöka och lösa alla klagomål inom en definierad tidperiod och även implementera nya lösningar för att förhindra att problemet återkommer.*

Upplands Väsby kommun har satsat på en kombination av aktiviteter för att göra sin ledning och sina anställda medvetna om deras förpliktelse att rapportera säkerhetsincidenter och

personuppgiftsincidenter. I kombinationen ingår utbildningsserien som hölls 2018 (se sektion 2.3.1, sida 14) och en informationssida på kommunens intranät. Sidan innehåller en definition av personuppgiftsincidenter och instruktioner på hur man ska agera vid misstanke om att en incident kan ha inträffat, samt en lista med information som ska ingå i rapporteringen.

För att hantera rapporterade incidenter har kommunen dokumenterat en incidenthanteringsprocess som definierar standardiserade steg i hanteringen av personuppgiftsincidenter. Den inkluderar aktiviteter som ska utföras av användare, hjälpdesken, den informationssäkerhetsansvarige och kommunens dataskyddsombud. I processkartan återfinns dock inte alla aktiviteter som under granskningens intervjuer beskrevs som en del av incidentprocessen; det saknas till exempel en aktivitet där man avgör om och hur registrerade som drabbas av incidenten ska få information om incidenten.

I processen dokumenterar och bedömer dataskyddsombudet däremot incidentens allvarlighet i Datainspektionens rapporterings- och utvärderingsmall. Svarsalternativ som medför att en incident ska rapporteras till tillsynsmyndigheten är tydligt markerade som sådana, vilket säkerställer att förpliktelsen att rapportera incidenter till DI prövas för varje incident. I och med att Upplands Väsby kommun använder Datainspektionens mall i rapporteringen till myndigheten är kraven om vilken information som ska ingå i rapporteringen uppfyllt.

Kommunen sparar alla incidentrapporter i dess ärendehanteringssystem, oavsett hur man bedömer incidentens allvarlighet eller om incidenten rapporteras till Datainspektionen. Ärendehanteringssystemet uppfyller funktionen som ett internt incidentregister. Dataskyddsfunktionen ska framöver använda registret för att utvärdera hur väl de interna instruktionerna efterlevs. Det är tänkt att dessa uppföljningar ska ske två gånger per år.

För att säkerställa att verksamheten över tid följer förändringar i lagkrav avseende incidenter, mottar dataskyddsfunktionen SKL:s och Datainspektionens nyhetsbrev och informationssessioner.

Observationer

Information till registrerade som drabbas av personuppgiftsincidenter ingår inte i processkartan för incidenthantering. Hittills har kommunen inte etablerat utvärderingar på hur väl dem interna incidentinstruktionerna efterlevs. Förändringar i lagkraven som gäller incidenthanteringen identifieras endast passivt via nyhetsbrev.

Rekommendationer

1. Inkludera alla relevanta aktiviteter och bedömningskriterier i rutinen som styr hur personuppgiftsincidenter ska hanteras och rapporteras till tillsynsmyndigheten inom 72 timmar.
2. Implementera en rutin som innebär att man följer upp hur väl de interna instruktionerna eller rutinerna efterlevs, vad gäller personuppgiftsincidenter.

2.7. Kontroll

2.7.1. Rapportering

Rapportering *syftar till att undersöka om verksamhetens rutiner, för hur intern rapportering till styrelse och ledning samt extern rapportering till datainspektionen sker rörande hur verksamheten, lever upp till lagkraven.*

Dataskyddsombudet lämnar en årlig rapport till kommunens och nämndernas ledning.

Rapporten täcker status i dataskyddsarbetet, till exempel information om brister som har identifierats eller om aktiviteter som föreslås för att åtgärda bristerna. Utöver detta saknas dock rutiner som säkerställer mer frekventa rapporter och ad-hoc rapportering till styrelsen och nämnderna. En bidragande faktor till detta är att styrelsen och nämnderna inte har satt tydliga förväntningar och krav på dataskyddsombudets och dataskyddsfunktionens rapportering.

Dataskyddsombudet är utsedd kontaktperson gentemot Datainspektionen för att svara på eventuella förfrågningar, och för att rapportera personuppgiftsincidenter.

Verksamheten har kommunicerat dataskyddsombudets namn och kontaktuppgifter till tillsynsmyndigheten. I nuläget har Upplands Väsby kommun inte etablerat en formell rutin för att svara på förfrågningar från Datainspektionen, utan detta sker ad-hoc beroende på förfrågningens typ och innehåll i vartenda särskilt fall. I och med att dokumentationen till varje personuppgiftsbehandling i Draftit Privacy är uppbyggd för att innehålla information om ansvarsområden, kontaktuppgifter, behandlingssyftet och skyddsåtgärder har kommunen goda förutsättningar för att kunna svara på Datainspektionens förfrågningar. Detta kräver dock att dokumentationen i registret är fullständig och uppdaterad (se tidigare rekommendationer).

Observationer

Det saknas en formell rutin för mer frekventa/ad-hoc rapporter till styrelse/nämnd och krav som sådan rapportering ska utgå ifrån. Det saknas en formell rutin för att svara på förfrågningar från Datainspektionen.

Rekommendationer

1. Fastställ rapporteringskrav gällande frekvens och innehåll som rapporteringen till styrelse/nämnd ska utgå ifrån.
2. Implementera en formell process, rutin, funktion eller motsvarande för att svara på förfrågningar från Datainspektionen.

Ø 3,3

Planeras

2 1

2.7.2. Granskning

Granskning *utforskar om verksamheten har någon plan på plats för att säkerställa (granska) att hanteringen av (känsliga) personuppgifter sker enligt krav (plan för integritetsgranskning).*
Det är fördelaktigt för verksamheter att genomföra regelbundna integritetsgranskningar för att identifiera riskområden eller potentiella brister, så att de kan hanteras och avhjälpas på lämpligt sätt.

Idag finns det ingen fastslagen granskningsplan för att utvärdera och säkerställa att kommunen uppfyller kraven på hantering av personlig information, särskilt angående känslig information. I nuläget har man endast planer att integrera dataskyddsarbetet i kommunens och nämndernas internkontrollarbete. Detta var tänkt att ske i samband med införandet av ett ledningssystem för informationssäkerhet. Införandet ligger dock på is efter informationssäkerhets-samordnaren som också hade funktionen som digitaliseringsdirektör har lämnat kommunen vid årsskiftet 2018/19. Som konsekvens av att man inte utför några granskningar enligt en fastslagen granskningsplan har man inte heller dokumenterat eller kommunicerat några granskningsresultat, utöver det som ingick i dataskyddsombudets egen rapport i januari 2019.

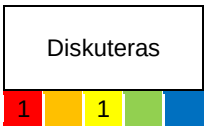
Observationer

Ø 2,0

Kommunen har ingen fastslagen granskningsplan eller internkontrollfunktion med fokus på dataskyddsarbetet och dataskyddsförordningens krav.

Rekommendationer

1. Inkludera dataskyddsarbetet i kommunens internkontrollarbete och kommunicera granskningarnas resultat till kommunens ledning/styrelse och nämnderna.



3. Bilaga: Källförteckning

1. Intervjuade roller

- Dataskyddsombud – Robert Åsberg
- Systemförvaltningschef – Stig Fjeldheim (Satt i styrgruppen för GDPR-projektet)

2. Dokumentation

- Dataskyddsombudets rapport 2018
- Slutrapport Projekt för anpassning till nya dataskyddsförordningen (GDPR)
- Informationssäkerhetspolicy (reviderad 2016-11-21, giltig t o m 2017-12-31)
- Riktlinjer för informationshantering (reviderad 2016-09-05, giltig t o m 2018-06-30)
- Informationssäkerhetspolicy (remissversion 2018-11-29)
- Riktlinjer informationssäkerhet (utkast)
- Arbetssteg för att hantera förfrågan
- Dokumentationen till personuppgiftsbehandlingen ”Språkkunnig personal i Upplands Väsby kommun” i Draftit Privacy
- Incidenthantering (processkarta)
- Anmälan av personuppgiftsincident (mall)
- Mall för den Personuppgiftsansvarige Instruktion för Behandling av Personuppgifter (mall)
- Upphandlingsprocessen (processkarta)
- Personuppgiftsbiträdesavtal (mall)
- Checklista vid upprättande eller granskning av personbiträdesavtal GDPR (mall)
- Mall för lista över underbiträden (mall)
- Förvaltningsplan 2019: Systemstöd för nämndadministration och kommunövergripande diarieföring
- Policy för förvaltningsmodell (utkast)
- Förvaltningsplan (mall)
- Kommunens gemensamma hanteringsanvisning (skärmdumpar från intranätet, som exemplarisk illustration)
- Personuppgiftsincidenter (skärmdump från intranätet)
- Informationssäkerhet (skärmdump från intranätet)
- Dataskyddsförordningen (GDPR) -> Roller – Funktioner (skärmdump från intranätet)
- Anmälan användning av massor eller avfall för anläggningsändamål (blankett)