Granskning av införande av GDPR

Hultsfreds kommun

December 2020

Caroline Liljebjörn

pwc

Revisionsrapport

Innehållsförteckning

Sammanfattning

Dataskyddsförordningen eller General Data Protection Regulation (GDPR) trädde i kraft inom EU:s samtliga medlemsländer 2018-05-25. En EU-förordning blir direkt tillämplig i medlemsländerna till skillnad från EU-direktiv. Genom att nya regler trädde i kraft upphörde nuvarande personuppgiftslag (PuL). Syftet med den nya förordningen är att skydda fysiska personers integritet vid behandling av personuppgifter.

Revisorerna i Hultsfreds kommun har, utifrån en bedömning av väsentlighet och risk, funnit det angeläget att granska om kommunstyrelsen och nämnderna vidtagit ändamålsenliga åtgärder vid införandet av dataskyddsförordningen.

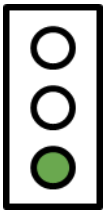
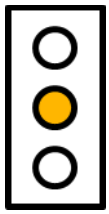
Syftet med granskningen är att säkerställa att kommunstyrelsen och nämnderna har vidtagit ändamålsenliga åtgärder vid införande av dataskyddsförordningen.

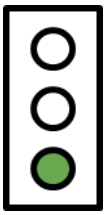
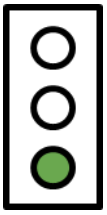
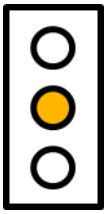
Efter genomförd granskning lämnas följande övergripande revisionella bedömning:

Vi bedömer att kommunstyrelsen och nämnderna inte helt har vidtagit ändamålsenliga åtgärder vid införande av dataskyddsförordningen.

Bedömningen grundas på avstämningen av revisionsfrågorna.

Bedömningar mot revisionsfrågor

Revisionsfrågor	Kommentar	
Upprätthålls tillräcklig säkerhet vid behandling av personuppgifter?	**Uppfyllt** Vi bedömer att det vidtagits både organisatoriska och tekniska åtgärder för att tillräcklig säkerhet vid behandling av personuppgifter ska upprätthållas. Det kvarstår att förtydliga vad uppdraget som kontaktperson består i.	
Finns rutiner för anmälan av personuppgifts-incidenter?	**Delvis uppfyllt** Vi bedömer att det finns en rutin för rapportering av personuppgiftsincidenter, men att den skulle behöva implementeras tydligare för att få fullt genomslag. Den information som finns på kommunens webb-sida är i vissa delar motsägelsefull, till exempel avseende till vem/vilka som en personuppgiftsincident ska rapporteras.	

Finns uppdaterade register över de behandlingar av personuppgifter som görs?	**Uppfyllt** Vi bedömer att det finns en dokumentation över de behandlingar av personuppgifter som görs. Det baserar vi på att arbetet påbörjades den initiala processen att kartlägga och dokumentera personuppgiftsbehandlingar har avslutats. Vi ser positivt på att konsekvensbedömningar kommer att påbörjas. Vi instämmer i synpunkten som framkommer att rutiner för att hålla dokumentationen aktuell behöver utarbetas. Det gäller både anmälan av nya personuppgiftsbehandlingar samt uppdatering och eventuellt borttag av befintlig dokumentation.	
Har dataskyddsombud utsetts?	**Uppfyllt** Vi bedömer att kommunstyrelsen och nämnderna har utsett dataskyddsombud, att besluten anmälts till Datainspektionen och att dataskyddsombudets kontaktuppgifter offentliggjorts på kommunens hemsida.	
Har tillräckliga åtgärder vidtagits för att säkerställa att förordningen följs?	**Delvis uppfyllt** Vi bedömer att åtgärder vidtagits som syftar till att säkerställa att förordningen följs. Samtidigt kvarstår åtgärder som att ta fram en övergripande policy för dataskydd, definiera ansvar och roller för kontaktpersonerna, ta fram rutiner och riktlinjer för hur dokumentation av personuppgifter ska hållas uppdaterad, dokumentera konsekvensanalyser och riskanalyser för de säkerhetsåtgärder som vidtas samt att upprätta rutiner för att kunna visa att förordningen följs.	

Finns det rutiner för att kunna visa att förordningen följs?	**Ej uppfyllt** Vi bedömer att det saknas rutiner för att kunna visa att förordningen följs. Det baserar vi på att det inte upprättats rutiner för att samla ”bevis” samtidigt som det kvarstår att utföra konsekvensanalyser och riskanalyser för de säkerhetsåtgärder som vidtas.

Rekommendationer

Vi rekommenderar kommunstyrelsen/nämnderna att:

- upprätta en övergripande policy för dataskydd som beskriver mål, styrning, organisation och ansvar för dataskyddsarbetet, till exempel vad gäller roller och ansvar för utsedda kontaktpersoner. För att avgränsningen mot dataskyddsombudets ansvar ska förtydligas, anser vi att kommunstyrelsen bör överväga att utse en av kontaktpersonerna som samordnare för arbetet med personuppgiftsfrågor.
- samordna rutinen för hantering av personuppgiftsincidenter och utse en eller flera personer som att ska se till att incidenter dokumenteras på rätt sätt, göra en bedömning om incidenten behöver anmälas och vid behov göra anmälan vilken enligt GDPR görs till Datainspektionen.
- inhämtade uppgifter om personuppgiftsbehandlingar struktureras i ett register, som hålls tillgängligt i elektronisk form.
- rutiner och riktlinjer tas fram för hur dokumentationen av personuppgiftsbehandlingar hålls uppdaterad, till exempel genom regelbunden genomgång utifrån vilka behandlingar som tillkommit, förändrats eller avslutats.
- genomföra planerade konsekvensanalyser och därefter utföra analyser till exempel vad gäller riskanalyser för säkerhetsåtgärder.
- upprätta rutiner för att samla ”bevis” för att kunna visa att förordningen följs.

Inledning

Bakgrund

Dataskyddsförordningen eller General Data Protection Regulation (GDPR) trädde i kraft inom EU:s samtliga medlemsländer 2018-05-25. En EU-förordning blir direkt tillämplig i medlemsländerna till skillnad från EU-direktiv. Genom att nya regler trädde i kraft upphörde nuvarande personuppgiftslag (PuL). Syftet med den nya förordningen är att skydda fysiska personers integritet vid behandling av personuppgifter.

Den nya förordningen bygger på tidigare regler på området, men innehåller också en del nyheter. En nyhet är att varje personuppgiftsansvarig som är en myndighet måste utse ett Dataskyddsombud.

Inom kommunen är varje myndighet (styrelse eller nämnd) personuppgiftsansvarig. Detta innebär att respektive styrelse eller nämnd är ansvarig för att de registrerades rättigheter upprätthålls. Ett förberedande arbete har behövts som innebär att förteckna personuppgiftsbehandlingar, bestämma ändamål och syfte med behandlingen, göra inventeringar för att se vilka lagliga grunder myndigheten har för sin behandling av personuppgifter.

Revisorerna i Hultsfreds kommun har, utifrån en bedömning av väsentlighet och risk, funnit det angeläget att granska om kommunstyrelsen och nämnderna vidtagit ändamålsenliga åtgärder vid införandet av dataskyddsförordningen.

Syfte och Revisionsfrågor

Syftet med granskningen är att säkerställa att kommunstyrelsen och nämnderna har vidtagit ändamålsenliga åtgärder vid införande av dataskyddsförordningen.

- Upprätthålls tillräcklig säkerhet vid behandling av personuppgifter?
- Finns rutiner för anmälan av personuppgiftsincidenter?
- Finns uppdaterade register över de behandlingar av personuppgifter som görs?
- Har dataskyddsombud utsetts?
- Har tillräckliga åtgärder vidtagits för att säkerställa att förordningen följs?
- Finns det rutiner för att kunna visa att förordningen följs?

Revisionskriterier

- Dataskyddsförordningen (General data protection regulation, GDPR)
- Reglementen för kommunstyrelsen och nämnderna
- Övriga kommunala styrdokument såsom policyer/riktlinjer och rutiner med bäring på granskningsområdet.

Avgränsning

Granskningen avgränsas till kommunstyrelsen, barn- och utbildningsnämnden samt

socialnämnden.

Metod

Vi har tagit del av följande dokument: gemensamt reglemente för kommunstyrelsen, barn- och utbildningsnämnden samt socialnämnden, delegationsordning kommunstyrelsen, delegationsordning barn- och utbildningsnämnden, delegationsordning socialnämnden, ruiner och blanketter för hantering av personuppgifter inom barn- och utbildningsnämnden och socialnämnden.

Vi har genomfört intervjuer med följande: ordförande i kommunstyrelsen, ordföradnde i barn- och utbildningsnämden, ordförande i socialnämnden, dataskyddsombud, kontaktpersoner i dataskyddsfrågor inom kommunstyrelsen, barn- och utbildningsnämnden samt socialnämnden och IT-chef.

Samtliga intervjuade har beretts möljighet att granska faktauppgifterna i rapporten. Rapporten har justerats utifrån inkomna synpunkter.

Iakttagelser och bedömningar

För varje revisionsfråga redogörs för vilka iakttagelser och revisionella bedömningar som gjorts. I inledningen av varje revisionsfråga anges vilken artikel i förordningen som är tillämpbar.

Upprätthålls tillräcklig säkerhet vid behandling av personuppgifter?

Iakttagelser

Artikel 32:

1. *Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är tillämpligt*
   - *a) Pseudonymisering och kryptering av personuppgifter*
   - *b) Förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet, och motståndskraft hos behandlingsystemen och tjänsterna*
   - *c) Förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk och teknisk incident*
   - *d) Ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.*

Enligt förordningen artikel 32 ska den personuppgiftsansvarige och dess biträde vidta lämpliga åtgärder både vad gäller organisation och teknik för att säkerställa ett skydd för personuppgifter. Ovan anges i punktform vad skyddet kan innebära.

Organisatoriska åtgärder

I dataskyddsförordningen finns ansvar beskrivet för olika roller, som är inblandade i behandlingen av personuppgifter. Personuppgiftsansvarig är den myndighet som bestämmer för vilka ändamål personuppgifterna ska behandlas och hur behandlingen ska gå till. Det åligger den personuppgiftsansvarige att se till att behandlingen sker i enlighet med dataskyddsförordningens bestämmelser. Enligt det gemensamma reglementet för kommunstyrelsen, barn- och utbildningsnämnden samt socialnämnden är styrelsen och nämnderna personuppgiftsansvariga för de register och andra behandlingar av personuppgifter som sker inom respektive verksamhet.

Enligt delegationsordningen för kommunstyrelsen ansvarar ordförande för att besluta om nya eller förändrade behandlingar enligt dataskyddsförordningen inom kommunstyrelsens enheter.

Enligt delegationsordningen för barn- och utbildningsnämnden är det

förvaltningschefen som beslutar att ingå personuppgiftsbiträdesavtal med personer utanför den kommunala organisationen, vilka behandlar personuppgifter för barn- och utbildningsnämndens räkning. Vidare beslutar förvaltningschefen om den registrerades rättigheter i fråga om rättelse, radering, begränsning av behandling och överföring av personuppgifter till annan personuppgiftsansvarig (så kallad dataportabilitet).

Enligt delegationsordningen för socialnämnden ansvarar ordförande för att besluta om nya eller förändrade behandlingar enligt dataskyddsförordningen inom socialnämndens enheter. Tecknande av avtal som inte beslutats av socialnämnden eller arbetsutskott delegeras till förvaltningschefen.

Det är personuppgiftsansvarig som utser dataskyddsombud (se vidare avsnitt Dataskyddsombud). Utöver dataskyddsombud har kontaktpersoner för dataskyddsfrågor utsetts inom respektive förvaltning. I intervjuerna framkommer att det saknas en tydlig beskrivning som anger vad kontaktpersonernas uppdrag består i. Det saknas även avgränsning mot dataskyddsombudets ansvarsområde.

Övriga förberedelser innan förordningen trädde i kraft

I januari 2017, det vill säga mer än ett år innan dataskyddsförordningen trädde i kraft, påbörjade tillträdande dataskyddsombudet och dåvarande personuppgiftsbiträde att förbereda införandet av GDPR. Förberedelserna omfattade bland annat att gå på utbildningar och att arrangera utbildningar för tjänstemän och förtroendevalda samt att förbereda verksamheterna inför upprättandet av registerförteckningar av personuppgiftsbehandlingar och personuppgiftsbiträdesavtal med leverantörer. I intervju beskriver dataskyddsombudet att erhållen utbildning varit tillräcklig för rollen.

Dataskyddsombudet besökte inför införandet av förordningen kommunfullmäktige för att presentera sig och svara på frågor. Det har även arrangerats utbildningar för förtroendevalda, men de ordföranden som intervjuats förklarar att de inte hade möjlighet att närvara.

Kommunstyrelsen

På kommunens hemsida finns information om vilka rättigheter som kommunmedborgare har vad gäller behandling av personuppgifter.[1] Det finns en överenskommelse om att den kommunövergripande informationen gäller för samtliga nämnder.

Inom både kommunstyrelsen och nämnderna har det genomförts ett arbete att identifiera leverantörer som för kommunens räkning behandlar personuppgifter. I dessa fall har personuppgiftsbiträdesavtal upprättats

[1] https://www.hultsfred.se/artikel/behandling-av-personuppgifter/

Socialnämnden

På kommunens hemsida finns information om hur socialförvaltningen skyddar personuppgifter hos dem som söker insatser.[2]

I intervju beskrivs att vanan att hantera känslig information är stor inom verksamheten, men att arbetet med införande av GDPR har gjort att information som behandlas har belysts. Personalen har till exempel fått ytterligare utbildning i vilka personuppgifter som behöver sparas i dokumentationen. Systemansvarig för verksamhetssystemet Treserva deltog i förberedelserna inför förordningens inträdande. Det påbörjades gallring av uppgifter i systemet vilket inte hade gjorts tidigare. I övrigt sker gallring enligt beslutad dokumenthanteringsplan.

Material har tagits fram för att informera de registrerade inom socialnämndens verksamhetsområden på vilken grund som personuppgifterna registreras.

Barn- och utbildningsnämnden

Inför att förordningen trädde i kraft tog kontaktpersonen för barn- och utbildningsförvaltningen fram riktlinjer och blanketter för hantering av personuppgifter i verksamheten. Det finns ett dokument från mars 2018 som innehåller regler för behandling av personuppgifter inom nämndens verksamheter. Dokumentet innehåller riktlinjer om säkerhet, särskilt känsliga uppgifter, samtycke, gallring, incidentrapporter samt anmälan av behandling av personuppgifter.

Vidare finns riktlinjer för behandling av personuppgifter i verksamhetssystemen Informentor och IST-Extens. Riktlinjer innehåller bland annat plan för gallring av personuppgifter i systemen. Material har tagits från för att informera vårdnadshavare och barn/elever inom förskola, skola och vuxenutbildning på vilken grund som personuppgifterna registreras.

Det finns även riktlinjer för hantering av barn och elever med skyddade personuppgifter samt en handlingsplan för hur skyddet kring dessa ska upprätthållas.

Dokumenten finns på barn- och utbildningsförvaltningens webb-sida under blanketter och e-tjänster.

Tekniska åtgärder

Ungefär samtidigt som GDPR infördes gick kommunen över till Office 365 som är en molnbaserad digital plattform för kommunikation, samarbete och mobilitet. Dataskyddsombudet var delaktig i diskussionerna vid införandet för att ta ställning till hanteringen av personuppgifter och därtill kopplad känslig information.

Med Office 365 följer ett antal verktyg för hantering av personuppgifter. Verktygen har i de flesta fallen inte aktiverats. Om någon vill veta vilka uppgifter som finns registrerade inom Hultsfreds kommun finns det ett verktyg som skapar en lista med dokument som personuppgifterna finns i. Verktyget har endast testkörts, men kan

[2] https://www.hultsfred.se/artikel/information-om-behandling-av-personuppgifter-inom-socialtjansten/

aktiveras om en förfrågan inkommer. I intervju beskrivs att Office 365 medfört större möjligheter att efterleva GDPR än tidigare.

Förmågan att återställa tillgänglighet hanteras via dagliga backuper. Backuper för Office 365 görs vid varje förändring och sparas i tio år medan backuper för lokala system sker en gång per natt och sparas i fem år. Det finns en rutin som innebär att backuperna testkörs enligt schema.

Bedömning

Vi bedömer att det vidtagits både organisatoriska och tekniska åtgärder för att tillräcklig säkerhet vid behandling av personuppgifter ska upprätthållas. Åtgärder som införts innebär bland annat att upprätta en organisation med personuppgiftsansvarig, dataskyddsombud och kontaktperson, att genomföra informationsinsatser inför införandet av förordningen, att upprätta informationstexter, riktlinjer och blanketter samt att ytterligare se över dokumentationen av extra känslig information. Vi bedömer att övergången till Office 365 bidragit till att underlätta efterlevanden av GDPR, till exempel avseende utsökning av information efter förfrågan.

Det kvarstår att förtydliga vad uppdraget som kontaktperson består i. Vi rekommenderar att någon av kontaktpersonerna utses som samordnare för att en enhetlig hantering av personuppgiftsfrågorna i kommunen ska säkerställas.

Revisionsfrågan bedöms som uppfylld.

Finns rutiner för anmälan av personuppgiftsincidenter?

Iakttagelser

> *Artikel 33:*
>
> *Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig i enlighet med artikel 55, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om anmälan till tillsynsmyndigheter inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.*

Varje personuppgiftsansvarig (nämnd, förbund eller styrelse) ansvarar för att åtgärda, dokumentera och eventuellt anmäla personuppgiftsincidenter. Den personuppgiftsansvarige bör därför utse en eller flera personer som ska se till att incidenter dokumenteras på rätt sätt, gör en bedömning om incidenten behöver anmälas och vid behov göra anmälan vilken enligt GDPR görs till Datainspektionen.

Dataskyddsombudet har tagit fram en rutin för anmälan av personuppgiftsincidenter och en blankett för anmälan. Blanketten innehåller frågor om de uppgifter som Datainspektionen efterfrågar vid anmälan om en personuppgiftsincident. De utsedda kontaktpersonerna har informerats om rutinen och i personalbladet i juni 2019 kunde anställda i Hultsfreds kommun bland annat läsa om vilka åtgärder som behöver vidtas om en personuppgiftsincident inträffar. Alla personuppgiftsincidenteter ska rapporteras så snart som möjligt efter upptäckt till närmaste chef, nämndens kontaktperson eller dataskyddsombudet. Den som tar emot anmälan gör en bedömning av incidentens

allvarlighetsgrad och avgör om anmälan behöver ske till Dataskyddsinspektionen, vilket ska ske inom 72 timmar från upptäckten. I samband med artikeln i personalbladet fanns en blankett för anmälan av personuppgiftsincident.

Anställda inom barn- och utbildningsnämndens verksamheter kan hitta information på kommunens hemsida om anmälan om personuppgiftsincidenter. Även här finns information om vad en personuppgiftsincident är och vilka åtgärder som ska vidtas om en personuppgiftsincident inträffar. Instruktionerna skiljer sig från de som fanns i personalbladet (juni 2019) genom att varje person som läser informationen förutsätts dokumentera incidenten och anmälan den till Datainspektionen. Enligt uppgift kan dataskyddsombudet i nödfall kontaktas för hjälp med bedömningen. Det finns en länk till Datainspektionens sida om personuppgiftsincidenter. Blanketten för anmälan av personuppgiftsincident finns bland nämndens övriga blanketter och e-tjänster.

Anställda inom socialnämndens verksamheter kan hitta information om anmälan av personuppgiftsincident på intranätet. Rutinen överensstämmer med den som beskrivs för barn- och utbildningsförvaltningen.

I intervju beskrivs att rutinen behöver implementeras tydligare för att fungera fullt ut. Hittills har endast två incidentrapporter kommit in. Ingen anmälan har behövt göras till Datainspektionen.

Bedömning

Vi bedömer att det finns en rutin för rapportering av personuppgiftsincidenter, men att den skulle behöva implementeras tydligare för att få fullt genomslag. Den information som finns på kommunens webb-sida är i vissa delar motsägelsefull, till exempel avseende till vem/vilka som en personuppgiftsincident ska rapporteras.

Vi rekommenderar kommunstyrelsen och nämnderna att samordna rutinen och utse en eller flera personer för hantering av personuppgiftsincidenter som att ska se till att incidenter dokumenteras på rätt sätt, gör en bedömning om incidenten behöver anmälas och vid behov göra anmälan vilken enligt GDPR görs till Datainspektionen.

Revisionsfrågan bedöms som delvis uppfylld.

Finns uppdaterade register över de behandlingar av personuppgifter som görs?

Iakttagelser

> *Artikel 30:*
>
> *1. Varje personuppgiftsansvarig och, i tillämpliga fall, dennes företrädare ska föra ett register över behandling som utförts under dess ansvar.*
>
> *2. Varje personuppgiftsbiträde och, i tillämpliga fall, dennes företrädare ska föra ett register över alla kategorier av behandling som utförts för den personuppgiftsansvariges räkning.*

Artikel 30 stadgar vad registret ska innehålla, att registret ska upprättas i elektronisk form och att det på begäran ska göras tillgängligt för tillsynsmyndigheten. Registret behöver bara upprättas om organisationen sysselsätter över 250 personer, såvida inte

den behandling som utförs kommer att medföra en risk för de registrerades rättigheter och friheter.

Inför införandet av förordningen tog SKR fram en mall för dokumentation av behandling av personuppgifter. Inom Hultsfreds kommun påbörjades arbetet att förteckna personuppgiftsbehandlingar under år 2017 vilket innebar att SKR:s mall inte fanns framtagen. Dokumentationen skedde istället på en blankett som togs fram för ändamålet. Blanketten innehåller uppgifter om ansvarig nämnd, behandlingens benämning, ändamålet med behandlingen, vilka som berörs av behandlingen, vilka personuppgifter som ska behandlas, till vilka mottagare uppgifterna kan komma att lämnas ut, åtgärder som vidtagits för att skydda säkerheten i behandlingen, när och hur gallring ska ske samt på vilken laglig grund som personuppgifterna samlas. På blankettens baksida finns en kort beskrivning av vilka uppgifter som ska fyllas i under varje punkt. Blanketten ska undertecknas av kommunstyrelsens/nämndens ordförande och skickas till dataskyddsombudet.

I intervju beskrivs att det varit ett stort projekt att inhämta dokumentation av samtliga behandlingar av personuppgifter. Dataskyddsombudet och kontaktpersonen för kommunstyrelsen besökte verksamheterna inom kommunhuset för att informera om behovet av dokumentation och alla anställda fick i uppgift att inventera förekomsten av personuppgiftsbehandlingar. Blanketterna med behandlingar skickades in till dataskyddsombudet och kontaktpersonen för kommunstyrelsen vilka gick igenom dokumentationen och skickade tillbaka blanketten för ändring och komplettering av lämnade uppgifter. I intervju beskrivs att arbetet tagit tid, men att den inledande dokumentationen nu är färdigställd. Det har inte tillsatts några extra resurser för att hantera arbetsmängden för den inledande dokumentationen. I intervju görs bedömningen att arbetsuppgifterna kopplade till införandet av GDPR kan ha trängt undan andra uppgifter som inte blivit gjorda eller som gjorts senare än normalt.

Insamlade blanketter har skannats samtidigt som originalen förvaras i pärmar. Kontaktpersonerna för barn- och utbildningsnämnden och socialnämnden har lagt in filerna i ärendehanteringssystemet Evolution. Vid granskningstillfället hade barn- och utbildningsnämnden 89 och socialnämnden 97 personuppgiftsbehandlingar dokumenterade. Kontaktpersonen för kommunstyrelsen har skannat blanketterna per förvaltning (totalt tolv) inom kommunstyrelsen. I intervju beskrivs att det inte finns några planer på att föra över dokumentationen till registerform eller liknande.

Det finns en viss osäkerhet att samtliga personuppgiftsbehandlingar som utförs inom kommunen blivit dokumenterade. Osäkerheten ökar ju längre ut i organisationen som verksamheten finns. I vintras besökte dataskyddsombudet kommunens förskolor för att informera om hanteringen av personuppgifter. Besöken upphörde när Coronapandemin bröt ut.

Hittills har dokumentationen över personuppgiftsbehandlingar hållits aktuell genom att det tillkommer nya behandlingar då och då som anmäls av ansvariga i verksamheten, men i intervju beskrivs att det behöver utarbetas tydligare rutiner för en regelbunden genomgång av dokumenterade behandlingar.

Det kvarstår att genomföra konsekvensbedömningar av de

personuppgiftsbehandlingar som dokumenterats. Konsekvensbedömningen är en process för att ta reda på vilka risker som finns med att behandla personuppgifter, ta fram rutiner och åtgärder för att bemöta dessa risker samt visa att dataskyddsförordningens krav uppfylls. I intervju beskrivs att konsekvensbedömningarna kommer att utföras under år 2021.

En annan stor uppgift har varit att samla in personuppgiftsbiträdesavtal från kommunens leverantörer. I samband med att förordningen trädde i kraft skickade övervägande del av berörda leverantörer in avtalsförslag. De som inte kontaktade kommunen självmant har dataskyddsombudet och kontaktpersonerna hört av sig till. Dataskyddsombudet har påmint verksamhetsföreträdare att efterfråga avtal med de leverantörer som tillkommer efter genomgången. Kommunen använder SKR:s mall för personuppgiftsbiträdesavtal.

Bedömning

Vi bedömer att det finns en dokumentation över de behandlingar av personuppgifter som görs. Det baserar vi på att den initiala processen att kartlägga och dokumentera personuppgiftsbehandlingar har avslutats. Vi ser positivt på att konsekvensbedömningar kommer att påbörjas.

Vi instämmer i synpunkten som framkommer att rutiner för att hålla dokumentationen aktuell behöver utarbetas. Det gäller både anmälan av nya personuppgiftsbehandlingar samt uppdatering och eventuellt borttag av befintlig dokumentation.

Vi rekommenderar att inhämtade uppgifter struktureras i ett register, som hålls tillgängligt i elektronisk form.

Revisionsfrågan bedöms som uppfylld.

Har dataskyddsombud utsetts?

Iakttagelser

> *Artikel 37:*
>
> *1. Den personuppgiftsansvarige och personuppgiftsbiträdet ska under alla omständigheter utnämna ett dataskyddsombud om*
>
> *a) behandlingen genomförs av en myndighet eller ett offentligt organ, förutom när detta sker som en del av domstolarnas dömande verksamhet,……..*
>
> *----*
>
> *7. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till tillsynsmyndigheten.*

Dataskyddsombudets uppgifter är enligt förordningen att informera och ge råd till den personuppgiftsansvarige, att övervaka efterlevnaden av förordningen, att ge råd om

behandling av personuppgifter vid införande av ny teknik samt att samarbeta med Datainspektionen.[3]

Kommunstyrelsen och nämnderna har tagit beslut om att utse Felicia Kurjenkallio till dataskyddsombud[4]. Besluten har därefter anmälts till Datainspektionen. I bekräftelsen står det angivet att dataskyddsombudets kontaktuppgifter ska offentliggöras, vilket skett på kommunens hemsida.

I intervju beskrivs att dataskyddsombudet även utsetts för Hultsfreds kommunala industriaktiebolag samt för Östra Smålands kommunalteknikförbund. Hittills har ombudets arbete främst inriktats på att utforma blanketter, informera om förordningen samt ge råd och stöd till kontaktpersonerna. Närmast förestående är att genomföra en snabbgranskning av dokumentationen som upprättats över behandling av personuppgifter. Granskningen kommer att inriktas på om dokumenterade uppgifter uppfyller förordningen. Det kommer även ske en bedömning om det saknas dokumentation av vissa behandlingar av personuppgifter.

Bedömning
Vi bedömer att kommunstyrelsen och nämnderna har utsett dataskyddsombud, att besluten anmälts till Datainspektionen och att dataskyddsombudets kontaktuppgifter offentliggjorts på kommunens hemsida.

Revisionsfrågan bedöms som uppfylld.

Har tillräckliga åtgärder vidtagits för att säkerställa att förordningen följs?

Iakttagelser
Som stöd i arbetet med att införa förordningen har SKR tagit fram en checklista som innehåller åtta punkter som SKR rekommenderade att alla kommuner gick igenom inför att förordningen började gälla. Vi stämmer av punkterna nedan mot de iakttagelser som vi gjort i samband med granskningen.

1. Förbered verksamheten

Inför att dataskyddsförordningen skulle träda i kraft genomfördes ett antal informationstillfällen för förtroendevalda i styrelse och nämnder samt för anställda i olika positioner. Tidigt identifierades behovet att förteckna personuppgiftsbehandlingar och upprätta personuppgiftsbiträdesavtal med leverantörer.

2. Organisera GDPR-arbetet

Granskade personuppgiftsansvariga myndigheter (styrelsen och nämnderna) har utsett dataskyddsombud. Det har även utsetts kontaktpersoner för förvaltningarna. Det kvarstår att tydliggöra ansvar och roller för kontaktpersonerna.

[3] Förordningen artikel 39
[4] KS § 34/2018-03-06, BUN § 30/2018-03-14 samt SN § 29/2018-03-14

3. Kartlägg

Granskningen visar att den initiala inventeringen och dokumentationen av hanteringen av personuppgifter har färdigställts. Det gäller även upprättandet av dokumentation över personuppgiftsbehandlingar.

Rutiner och instruktioner behöver tas fram för hur dokumentationen ska hållas kontinuerligt uppdaterad.

4. Analysera

I samband med att kartläggningen och dokumentationen som genomfördes ingick även att fastställa vilka rättsliga grunder som tillåter att respektive personuppgift får behandlas. Det kvarstår att utföra konsekvensanalyser vid behandlingar med särskilda integritetsrisker, t ex hälsa, etniskt ursprung, politisk uppfattning, medlemskap i fackförening etc.

5. Dokumentera

Det behövs en övergripande policy för dataskydd som beskriver mål, styrning, organisation och ansvar för dataskyddsarbetet. För närvarande saknas det övergripande policy eller riktlinjer för dataskyddsarbetet.

Dataskyddsförordningen ställer krav på att den personuppgiftsansvariga dokumentationen ska kunna visa att reglerna följs och hur reglerna följs. Det kräver förutom förteckningen av personuppgiftsbehandlingar och konsekvensanalyser även att det dokumenteras fler analyser till exempel vad gäller riskanalyser för säkerhetsåtgärder. I intervju beskrivs att det kvarstår att upprätta rutiner för att visa hur reglerna följs vad gäller konsekvensanalyser och riskanalyser för säkerhetsåtgärder.

6. Inför nya rutiner

Organisationen ska kunna upprätthålla ett långsiktigt arbete kring dataskydd. Det har till exempel skett en uppdatering av introduktionen av nyanställda samt dokumenthanteringsplaner. Dataskyddsombudet arbetar tillsammans med informationssäkerhetssamordnaren.

I samband med installering av Office 365 infördes verktyg för hantering av personuppgifter, till exempel för utsökning av uppgifter efter förfrågan. Andra områden som kan behöva ses över är upphandling, systemförvaltning och IT-drift.

7. Leverantörer och avtal

Det har genomförts en översyn av befintliga avtal inom både kommunstyrelsen och nämnderna vad gäller att upprätta personuppgiftsbiträdesavtal. Kontakt har tagits med leverantörer för att säkerställa att kunskap om det nya regelverket finns och att det finns samstämmighet om roller och ansvarsfördelning.

8. Säkerställ individens rättigheter

Granskningen visar att kommunstyrelsen har information på hemsidan som visar hur personuppgifter behandlas i verksamheten. Det finns även information hur individer ska begära att få tillgång till sina personuppgifter och få felaktiga personuppgifter rättade samt i förekommande fall raderade. Den kommunövergripande informationen gäller även övriga nämnder.

Bedömning

Vi bedömer att åtgärder vidtagits som syftar till att säkerställa att förordningen följs. Samtidigt kvarstår åtgärder som att ta fram en övergripande policy för dataskydd, definiera ansvar och roller för kontaktpersonerna, ta fram rutiner och riktlinjer för hur dokumentationen av personuppgifter ska hållas uppdaterad, dokumentera konsekvensanalyser och riskanalyser för de säkerhetsåtgärder som vidtas samt att upprätta rutiner för att kunna visa att förordningen följs.

Revisionsfrågan bedöms som delvis uppfylld.

Finns det rutiner för att kunna visa att förordningen följs?

Iakttagelser

> *Artikel 42:*
>
> 1. *Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning. Dessa åtgärder ska ses över och uppdateras vid behov.*

Det är den personuppgiftsansvarige som behöver kunna visa att åtgärder har vidtagits som ligger i linje med förordningen, det vill säga som har bevisbördan. Det kan till exempel göras genom att åtgärder som vidtas även dokumenteras i syfte att utgöra ”bevis” på att förordningen följs. I intervju beskrivs att det kvarstår att upprätta rutiner för att visa hur reglerna följs såväl som konsekvensanalyser och riskanalyser för säkerhetsåtgärder. Däremot finns dokumenthanteringsplaner för kommunstyrelsen och samtliga nämnder. Det gäller dock att kunna visa att dokumenhanteringsplanerna följs avseende rensning av data.

Bedömning

Vi bedömer att det saknas rutiner för att kunna visa att förordningen följs. Det baserar vi på att det inte upprättats rutiner för att samla ”bevis” samtidigt som det kvarstår att utföra konsekvensanalyser och riskanalyser för de säkerhetsåtgärder som vidtas.

Revisionsfrågan bedöms som ej uppfylld.

2020-12-14

Caroline Liljebjörn

Uppdragsledare/Projektledare

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av Hultsfreds kommun enligt de villkor och under de förutsättningar som framgår av projektplan från den 21 april 2020. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.