

Dataskyddssombudets årsrapport
Ellen Bäckman
2025-03-31

Dataskyddssombudets årsrapport 2024

Innehållsförteckning

1	Inledning	3
2	Sammanfattning och rekommendationer	3
3	Informationssäkerhets- och dataskyddsorganisationen	4
3.1	Ledningssystem och förutsättningar	4
4	Personuppgiftsincidenter	5
5	Revisioner	6
5.1	Kamerabevakning	6
6	Konsekvensbedömningar avseende dataskydd	6
7	Vägledning, stöd och rådgivning	7
8	Begäran och klagomål	7
9	Omvärldsbevakning	7
10	Dataskyddsombudets mål för 2025	7

1 Inledning

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU. Enligt dataskyddsförordningen är varje nämnd, styrelse och bolag inom Region Halland ansvarig för att verksamheten följer dataskyddslagstiftningen. Det innebär att dessa behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter. Varje nämnd, styrelse och bolag har utsett ett Dataskyddsombud (DSO). DSO:n har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå. I enlighet med artikel 38.3 i dataskyddsförordningen ska DSO rapportera om dataskyddsarbetet till den personuppgiftsansvariges högsta förvaltningsnivå, vilket sker genom denna årsrapport.

2 Sammanfattning och rekommendationer

Trots resursförstärkning inom avdelningen för Informationssäkerhet så är informationssäkerhetsspecialisterna, inriktning dataskydd, fortsatt överbelastade med ärenden och övriga dataskyddsfrågor. Att Region Hallands verksamheter har många dataskyddsfrågor och ärenden så som framtagandet av konsekvensbedömningar är en naturlig konsekvens av att Region Halland aktivt arbetar med att vara i digital framkant, men det medför många komplexa ärenden som behöver hanteras med stöd av dataskyddsfunktionen på ITD. Om Region Halland även fortsättningsvis vill vara i framkant gällande t.ex. AI-lösningar och molnlösningar kommer det kräva ytterligare resurser på dataskyddsfunktionen för att inom rimlig tid kunna hantera denna typ av ärenden samtidigt som övriga dataskyddsarbetet ska hanteras, alternativt tydligare övergripande samordning och prioritering kring vilka lösningar som ska införas och när.

Grundläggande förutsättningar för att på ett ansvarsfullt och strategiskt sätt bedriva informationssäkerhets- och dataskyddsarbete bedöms i vissa delar brista, dataskyddsombudet bedömer att det även fortsättningsvis måste prioriteras att säkerställa resurser och kompetens inom dessa området – och ansvarsfördelning måste vara tydlig. Vidare måste revidering av ledningssystemet även fortsatt prioriteras, den nu gällande styrdokumentationen inom området bedöms som svårbegriplig vilket med stor sannolikhet innebär att medarbetare inte vet eller förstår vad som förväntas av dem kopplat till informationssäkerhet- och dataskydd. Detta uttalande styrks av analysen av 2024 års personuppgiftsincidenter.

Även informationssäkerhetsspecialisterna, inriktning informationssäkerhet, bedöms vara underdimensionerade i förhållande till det som förväntas av dom. T.ex. pågår ett arbete med ny metod för att informationsklassificera regionens informationstillgångar, men det kan inte vara rimligt att anta att dessa resurser ska kunna driva det faktiska klassificeringsarbetet för hela regionens verksamheter.

Därtill tillkommer i närtid flera omfattande EU-lagstiftningar som kommer att innebära än mer arbete kopplat till informationssäkerhet, dataskydd och cybersäkerhet. NIS2 och AI-förordningen är exempel på sådan lagstiftning. Region Halland behöver dels utse vilken/vilka funktion/er som ska ansvara för hantering och rådgivning kopplat till dessa lagstiftningar, dels planera för eventuell resurs- och kompetenstillsättning.

Dataskyddsombudet vill till slut tydliggöra att trots att det finns brister och en hel del arbete att göra inom informationssäkerhet- och dataskyddsområdet så anser dataskyddsombudet att Regionen har goda förutsättningar för att hantera många av dessa frågor på ett bra sätt. Inom många verksamhetsområden bedömer dataskyddsombudet att det finns god förståelse för

säkerhetsfrågorna, och en stor vilja att skydda våra informationstillgångar. Det finns också i många fall väldigt goda exempel på välfungerande arbetsprocesser kopplat till t.ex. dataskyddsfrågorna som hanteras av Informationssäkerhetsavdelningen.

3 Informationssäkerhets- och dataskyddsorganisationen

Under 2024 har Region Halland fått ett nytt dataskyddsombud, som numera är organisatoriskt placerad på kansliavdelningen på Regionkontoret.

På avdelningen Informationssäkerhet, på IT och Digitalisering (ITD), har tre personer rekryterats under 2024 varav en ersatte en tidigare resurs som informationssäkerhetsspecialist. Av de övriga personerna är 1,5 heltider avsedd att förstärka dataskyddsarbetet som informationssäkerhetsspecialist inriktning dataskydd och 0,5 heltid ska förstärka informationssäkerhetsarbetet. I dagsläget arbetar 4,5 heltider med dataskydd och 2,5 heltider arbetar med informationssäkerhet inom Informationssäkerhetsavdelningen. Det är mycket positivt att dessa funktioner under 2024 har förstärkts med ytterligare resurser, men det är undertecknads åsikt att ytterligare förstärkning är nödvändig för att Region Halland på ett ansvarsfullt sätt ska kunna driva den digitala framfart och innovation som politiken har beslutat om.

Informationssäkerhetsspecialisterna, inriktning informationssäkerhet, har bland annat till uppgift att etablera systematiska arbetssätt för informationssäkerhet, praktiskt arbeta med ledningssystemet för informationssäkerhet, hantera workshops kopplat till informationsklassificering och riskanalyser samt agera rådgivande och vägledande för regionens verksamheter. De fungerar även samordnande mellan regionens övriga informationssäkerhetsresurser, idag har dock bara två av regionens förvaltningar utsedda informationssäkerhetsresurser utöver de som arbetar på Informationssäkerhetsavdelningen. Vidare har regionens signalskyddsorganisation sedan december 2024 placerats här, vilket ytterligare bidrar till ökad arbetsbelastning.

Informationssäkerhetsspecialisterna, inriktning dataskydd, har bland annat till uppgift att bistå regionens verksamheter samt politiska nämnder och ledning i dataskyddsfrågor för att uppfylla kraven i dataskyddsförordningen (GDPR) och tillhörande integritetslagstiftning. Rollen är både rådgivande och ett kunskapsstöd genom att vara förvaltningarnas kontaktperson när det gäller dataskydd. Det löpande arbetet består i huvudsak av att handlägga och utreda personuppgiftsincidenter, registrera och granska personuppgiftsbehandlingar samt stötta verksamheterna med att ta fram personuppgiftsbiträdesavtal (PUB-avtal) och konsekvensbedömningar avseende dataskydd (DPIA).

Dataskyddsombudet är en oberoende granskare och rådgivare avseende regionens dataskyddsarbete. Dataskyddsombudets arbete består i huvudsak av att övervaka den interna efterlevnaden av dataskyddsförordningen och annan dataskyddslagstiftning (genom bl.a. revisioner), granska DPIA's och lämna rekommendationer, genomföra utbildningar samt erbjuda löpande stöd och rådgivning inom organisationen.

Informationssäkerhetsavdelningen och dataskyddsombudet arbetar tätt ihop för att främja ett gott informationssäkerhets- och dataskyddsarbete inom Regionen.

3.1 Ledningssystem och förutsättningar

En viktig del av ett adekvat dataskydd förutsätter en god informationssäkerhetskultur och systematiskt informationssäkerhetsarbete, vilket följer av artikel 32 GDPR. Med anledning av detta har dataskyddsombudet också granskat ledningssystemet för informationssäkerhet- och dataskydd samt den övergripande nivån av regionens informationssäkerhetsarbete, och bedömer att det finns brister.

Dataskyddsbudeten bedömer att det nuvarande ledningssystemet är svårbegripligt för medarbetare, vilket kan vara en av anledningarna till att analysen av personuppgiftsincidenter visar att majoriteten av incidenter beror på felskick eller felregistrering. Styrdokumentet är därtill gamla och många hänvisningar/länkar fungerar inte. En översyn av styrdokumentationen inom informationssäkerhet- och dataskyddsområdet pågår redan hos Informationssäkerhetsavdelningen. Undertecknad vill lyfta att detta arbete fortsatt bör prioriteras och att nya styrdokument behöver förankras i verksamheterna.

Vidare pågår ett arbete med att införa ny metod för informationsklassificering inom regionen. Mot bakgrund av att något systematiskt informationsklassningsarbete inte har bedrivits de senaste åren, anser undertecknad att denna insats är nödvändig för att regionen ska kunna bedriva digitaliserings- och utvecklingsarbete på ett ansvarsfullt sätt. Förutsättningarna för att faktiskt utföra informationsklassificeringarna på ett systematiskt och fullgott sätt bör dock ses över, då det enligt dataskyddsbudeten bedömning inte är rimligt att anta att de befintliga 2,5 heltidsresurserna på Informationssäkerhetsavdelningen ska kunna driva detta arbete för alla regionens verksamheter.

4 Personuppgiftsincidenter

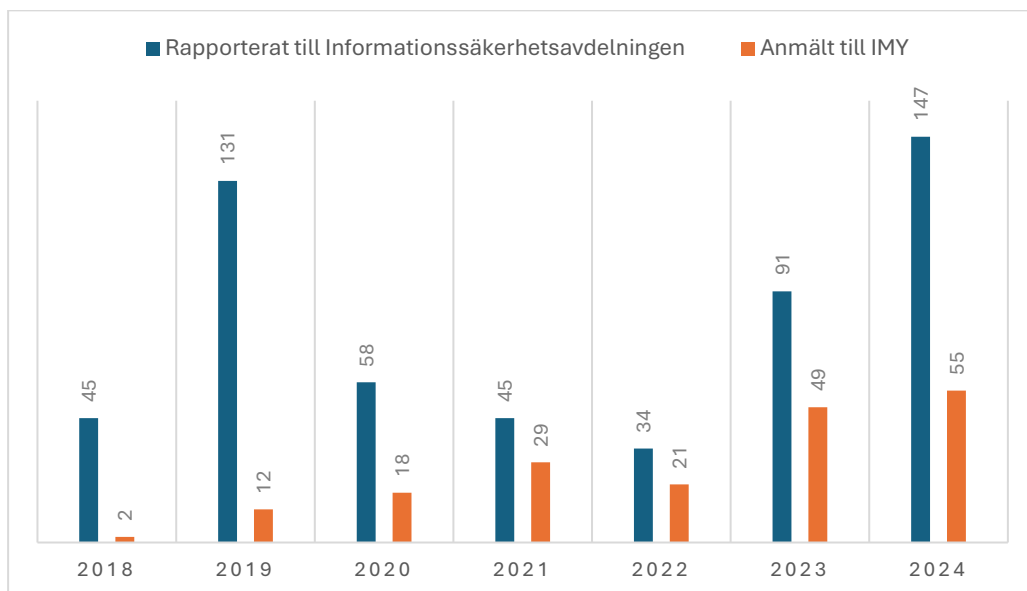
En personuppgiftsincident är en säkerhetsincident som leder till att personuppgifter förstörs, går förlorade, ändras eller kommer i orätta händer. Det har ingen betydelse om det har skett oavsiktligt eller med avsikt. Region Halland har en lagstadgad skyldighet att anmäla incidenter som kan innebära en risk för de registrerade till Integritetsskyddsmyndigheten inom 72 timmar. Vid höga risker finns det även en skyldighet att informera de registrerade om händelsen. Enligt Region Hallands rutiner rapporteras personuppgiftsincidenter till Informationssäkerhetsavdelningen som utreder ärendet. Dataskyddsbudeten bistår vid behov med råd avseende hantering av personuppgiftsincidenter.

Under 2024 har 147 personuppgiftsincidenter rapporterats, där regionen har bedömts vara personuppgiftsansvarig. Av dessa bedömdes 55 incidenter kunna innebära risk för den registrerade varför de anmäldes till Integritetsskyddsmyndigheten (IMY). IMY har i samtliga fall valt att ej vidta åtgärd.

Nedan anges antal personuppgiftsincidenter rapporterade per personuppgiftsansvarig nämnd, styrelse eller bolag.

Driftnämnd Hallands sjukhus	58
Driftnämnd Kultur och skola	1
Ambulans, diagnostik och hälsa	16
Driftnämnd Kollektivtrafik	0
Driftnämnd Psykiatri	26
Regionstyrelsen	11
Driftnämnd Närsjukvård	33
Driftnämnd Regionservice	2
Teater Halland AB	0

Tabellen nedan visar antalet inrapporterade personuppgiftsincidenter under åren 2018 till 2024. Orsaken till ökningen är okänd, men gissningsvis kan det bero på att det inom organisationen har blivit mer känt att incidenter ska rapporteras. Bilden visar också antalet som anmälts till IMY. Andelen anmälda incidenter till IMY har minskat, 2023 anmäldes cirka hälften av alla incidenter till IMY, 2024 har ca en tredjedel av alla incidenter anmälts till IMY. Orsaken till denna minskning är okänd.



Dataskyddombudet har analyserat de rapporterade incidenterna och kan konstatera att 103 av 147 incidenter avser felskickade handlingar eller felregistrering av uppgifter. För undertecknad skickar detta fynd en tydlig signal om att regionens styrning och stöd avseende informationshantering i stort måste ses över och på ett adekvat sätt förankras i verksamheterna. I detta ingår att säkerställa att det ledningssystem vi har inom informationssäkerhet och dataskydd är begripligt, korrekt och känt i verksamheten.

5 Revisioner

En av dataskyddsombudets huvuduppgifter är att övervaka Region Hallands efterlevnad av dataskyddsförordningen. Utförandet av detta uppdrag måste betraktas mot bakgrund av dataskyddsförordningens grundprincip om ansvarsskyldighet enligt vilken regionen måste kunna visa att reglerna i dataskyddsförordningen efterlevs. För att uppfylla principen om ansvarsskyldighet krävs att formaliserade interna dataskyddsrevisioner genomförs på ett systematiskt sätt.

5.1 Kamerabevakning

Föregående dataskyddsombud genomförde under 2024 en revision avseende kamerabevakning inom Region Halland. Sammantaget fann dataskyddsombudet att allvarliga brister fanns avseende Region Hallands personuppgiftsbehandling i samband med kamerabevakning. Det fanns bland annat pågående kamerabevakning utan erforderliga tillstånd samt brister kopplat till skyldigheten att föra register över pågående personuppgiftsbehandlingar (art. 30 GDPR). Undertecknad känner till att ett omfattande arbete har genomförts för att tydliggöra processen och hanteringen av kamerabevakning, och planerar att följa upp vidtagna åtgärder med anledning av denna revision under hösten 2025.

6 Konsekvensbedömningar avseende dataskydd

En konsekvensbedömning (DPIA) är en process för att identifiera och minimera risker för den personliga integriteten som uppstår i samband med en planerad personuppgiftsbehandling. Konsekvensbedömningen ska genomföras i de fall behandlingen av personuppgifter sannolikt leder till en hög risk för de registrerades fri- och rättigheter. Under 2024 har 14 konsekvensbedömningar slutförts och diarieförts inom Region Halland.

Personuppgiftsansvarig som bryter mot skyldigheten att göra en konsekvensbedömning riskerar att drabbas av sanktionsavgifter.

7 Vägledning, stöd och rådgivning

Rådgivning och utbildning är två av dataskyddsombudets centrala uppgifter. Dataskyddsombudet har, i stor omfattning, lämnat råd och stöd till informationssäkerhetsspecialisterna och till regionens olika verksamheter under året. Dataskyddsombudet har också handlagt ett antal frågor, lämnat rekommendationer på genomförda konsekvensbedömningar, träffat samtliga personuppgiftsansvariga och haft utbildning om GDPR samt stöttat Kommunikationsavdelningen på Regionkontoret i arbetet med att ta fram ny rutin och lathund avseende hantering av bild, film och ljudmaterial. Under våren 2025 har tre utbildningstillfällen till alla regionens kommunikatörer genomförts.

8 Begäran och klagomål

Region Hallands registrerade, som till exempel patienter och medarbetare, har rätt att inkomma med begäran om att utöva sina rättigheter under dataskyddsförordningen. Exempel på sådan begäran är att en patient eller medarbetare begär ut alla personuppgifter som är under behandling i regionen. Därutöver kan de registrerade komma in med klagomål och har även rätt att kräva skadestånd från Region Halland om de har lidit materiell eller immateriell skada till följd av en överträdelse av dataskyddsförordningen. Under 2024 har ett klagomål men inga begäran inkommit till det nya dataskyddsombudet från registrerade. Till Informationssäkerhetsavdelningen har inga begäran eller klagomål inkommit.

9 Omvärldsbevakning

2024 och den närmsta framtiden präglas av att EU-kommissionen släpper en stor mängd ny EU-reglering avseende digitalisering. De som primärt berör informationssäkerhet- och dataskyddsområdet är NIS2/cybersäkerhetslagen, AI-förordningen och möjligtvis Dataförordningen. Vidare har EHDS, det europeiska hälsodataområdet, som ställer krav på tillgängliggörande av hälsodata inom EU precis trätt i kraft. Dataskyddsombudet anser att även detta indikerar att regionen måste säkra resurser och kompetens för att kunna hantera dessa nya krav.

Vidare innebär oron i omvärlden att det är än mer angeläget att säkerställa ett gott skydd av vår data, inte minst gällande våra personuppgifter. Därtill finns det risk att överenskommelsen mellan EU-USA kan komma att hävas. Detta måste följas och Region Halland måste vara redo att agera, t.ex. genom att aktivera exit-planer, om vi inte längre kan använda de amerikanska lösningar vi har för personuppgiftsbehandling.

10 Dataskyddsombudets mål för 2025

Dataskyddsombudet har tagit fram en tillsynsplan och kommer under året genomföra revision mot tre personuppgiftsansvariga under året, en av dessa är redan utförd och kommer inom kort fastställas. Dataskyddsombudet kommer även fortsatt lägga mycket tid på att lära känna verksamheterna, bland annat genom att hålla riktade utbildningar.

Dataskyddsombudet tackar alla i regionen för ett gott samarbete under 2024 och hoppas på ett fortsatt gott samarbete under 2025.

Halmstad, den 31 mars 2025

Ellen Bäckman, dataskyddsombud