Dataskyddsombudets årsrapport 2025

Innehållsförteckning

1 Inledning

Dataskyddsförordningen (GDPR) 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 samt 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 och åtkomst 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 regionövergripande samordning och prioritering kring vilka lösningar som ska införas och när.

Även informationssäkerhetsspecialisterna, inriktning informationssäkerhet, bedöms vara underdimensionerade i förhållande till vad som förväntas utföras av informationssäkerhetsfunktionen. Som exempel kan det nämnas att funktionen sedan 2024 har arbetat med att införa en ny metod för att informationsklassificera regionens informationstillgångar, vilket är mycket positivt. Dock tycks det finnas en förväntan om att resurserna i fråga även ska driva det faktiska klassificeringsarbetet för hela regionens informationstillgångar, vilket enligt dataskyddsombudet inte bedöms som vare sig rimligt eller möjligt.

Grundläggande förutsättningar för att på ett ansvarsfullt och strategiskt sätt bedriva informationssäkerhets- och dataskyddsarbete bedöms i vissa delar brista. Dataskyddsombudet bedömer att regionen även fortsättningsvis behöver prioritera att säkerställa resurser och kompetens inom dessa området, och ansvarsfördelningen behöver tydliggöras. Idag saknas tydlig styrning avseende roller och ansvar inom detta område.

Revidering av ledningssystemet behöver, enligt dataskyddsombudet, fortsatt prioriteras. Den nu gällande styrdokumentationen inom området bedöms som svårnavigerad, svårbegriplig och i många fall utdaterad vilket kan antas medföra att medarbetare i många fall inte vet eller förstår vad som förväntas av dem kopplat till informationssäkerhet- och dataskydd. Denna bedömning styrks av analysen av 2024 och 2025 års personuppgiftsincidenter.

Flera omfattande EU-lagstiftningar har trätt i kraft eller kommer inom kort träda i kraft, som innebär mer arbete kopplat till informationssäkerhet, dataskydd och cyberssäkerhet. NIS2, som trätt i kraft i Sverige genom cybersäkerhetslagen i januari 2026, hanteras av informationssäkerhetsfunktionen. Även AI-förordningen är ett högaktuellt exempel på ny lagstiftning som behöver omhändertas innan den träder i kraft i stora delar augusti 2026.

Dataskyddsombudet bedömer att regionen omgående behöver utse vilken/vilka funktion/er som ska ansvara för hantering och rådgivning kopplat till denna lagstiftning samt planera för eventuell resurs- och kompetenstillsättning.

Dataskyddsombudet vill till slut tydliggöra att trots att det finns brister och utvecklingspotential inom informationssäkerhet- och dataskyddsområdet så bedömer dataskyddsombudet att regionen har goda förutsättningar för att hantera många av dessa frågor på ett systematiskt och rättssäkert 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 flera fall mycket goda exempel på välfungerande arbetsprocesser kopplat till t.ex. dataskyddsfrågorna.

3 Informationssäkerhets- och dataskyddsorganisationen

Under 2025 har en omorganisation på IT och Digitalisering (ITD) medfört att tidigare avdelning Informationssäkerhet numera heter avdelning Informationssäkerhet och åtkomst. På denna avdelning finns bland annat dataskyddsfunktionen och informationssäkerhetsfunktionen. På denna avdelning har en person rekryterats till dataskyddsfunktionen under 2025. Vid årsskiftet 2025/2026 fanns 5 heltider på dataskyddsfunktionen och 3 heltider på informationssäkerhetsfunktionen. Det är positivt att dessa funktioner under 2025 har förstärkts ytterligare, men det är dataskyddsombudets bedömning 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.

Informationssäkerhetsfunktionen har bland annat till uppgift att etablera systematiska arbetssätt för informationssäkerhet, praktiskt arbeta med ledningssystemet för informationssäkerhet, hantera informationsklassificering och riskanalyser samt agera rådgivande och vägledande för regionens verksamheter. Under slutet på 2025 och fortsatt in i 2026 arbetar funktionen aktivt med att säkerställa att kraven som följer av cybersäkerhetslagen (NIS2) omhändertas av regionen. Vidare har regionens signalskyddsorganisation sedan december 2024 placerats här.

Dataskyddsfunktionen har bland annat till uppgift att bistå regionens verksamheter samt politiska nämnder och ledning i dataskyddsfrågor för att uppfylla kraven i dataskyddsförordningen 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). Det står klart att funktionen tar emot fler ärenden än vad som rimligen kan hanteras av befintliga resurser, vilket i sin tur medför att verksamheterna många gånger får vänta i flera månader innan de kan få hjälp med sina ärenden. För att med digitala medel försöka effektivisera och förenkla handläggningen har funktionen i flera års tid efterfrågat ett systemstöd för denna handläggning, men detta behov har ledningen på ITD ännu inte har tillgodosett. Detta innebär att funktionen än i dag är tvungna att arbeta med föråldrade verktyg så som Word-mallar och Excel-filer. Dataskyddsombudet finner det anmärkningsvärt att det, i en tid då politiken tydligt uppmuntrar och efterfrågar smarta digitala lösningar för våra administrativa verksamheter, tycks finnas ett motstånd mot att tillse att lämpliga systemstöd för denna funktion införs.

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.

Informationssäkerhet- och dataskyddsfunktionerna 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 granskat ledningssystemet för informationssäkerhet- och dataskydd samt den övergripande nivån av regionens informationssäkerhetsarbete, och bedömer att det finns brister. Dessa brister uppmärksammades redan i 2024 års rapport.[1]

Dataskyddsombudet kan konstatera att avdelningen Informationssäkerhet och åtkomst har gjort vissa förändringar i ledningssystemet det senaste året, bland annat tagit fram en ny riktlinje. Det kan dock konstateras att det finns mycket kvar att revidera, bland annat har det lyfts att styrning kopplat till registerutdrag är bristfällig. Dataskyddsombudet bedömer således även detta år att det nuvarande ledningssystemet är svårnavigerat för medarbetare, vilket kan vara en bidragande faktor till att analysen av personuppgiftsincidenter visar att majoriteten av incidenter beror på felskick eller felregistrering. Många av styrdokumenten är därtill gamla och många hänvisningar/länkar fungerar inte. Arbetet med översyn av styrdokumentationen inom informationssäkerhet- och dataskyddsområdet går långsamt, och tycks återkommande nedprioriteras på grund av för hög belastning på informationssäkerhet- och dataskyddsfunktionerna. Dataskyddsombudet vill ännu en gång påpeka att detta arbete behöver prioriteras. I detta ingår att säkerställa att ledningssystemet är begripligt, korrekt och känt i verksamheten

En annan grundläggande del av informationssäkerhetsarbetet är att klassificera informationstillgångar, i syfte att få kontroll över hur olika tillgångar behöver skyddas eller hanteras utifrån aspekterna konfidentialitet, riktighet och tillgänglighet. Regionen har infört metoden KLASSA under 2024 och under 2025 har 21 klassificeringar av strukturerad information utförts. Under slutet av 2025 har man även påbörjat ett arbete för att använda ett systemstöd för att klassificera ostrukturerad information. Dataskyddsombudet bedömer det som mycket positivt att arbetet med informationsklassificeringar har kommit i gång, men vill lyfta att förutsättningarna för utförandet bör ses över då det inte bedöms rimligt att tre heltidsresurser ska kunna ansvara för och driva detta arbete för hela regionens informationstillgångar vid sidan av sina övriga arbetsuppgifter.

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 dataskyddsfunktionen som utreder ärendet. Dataskyddsombudet bistår vid behov med råd avseende hantering av personuppgiftsincidenter.

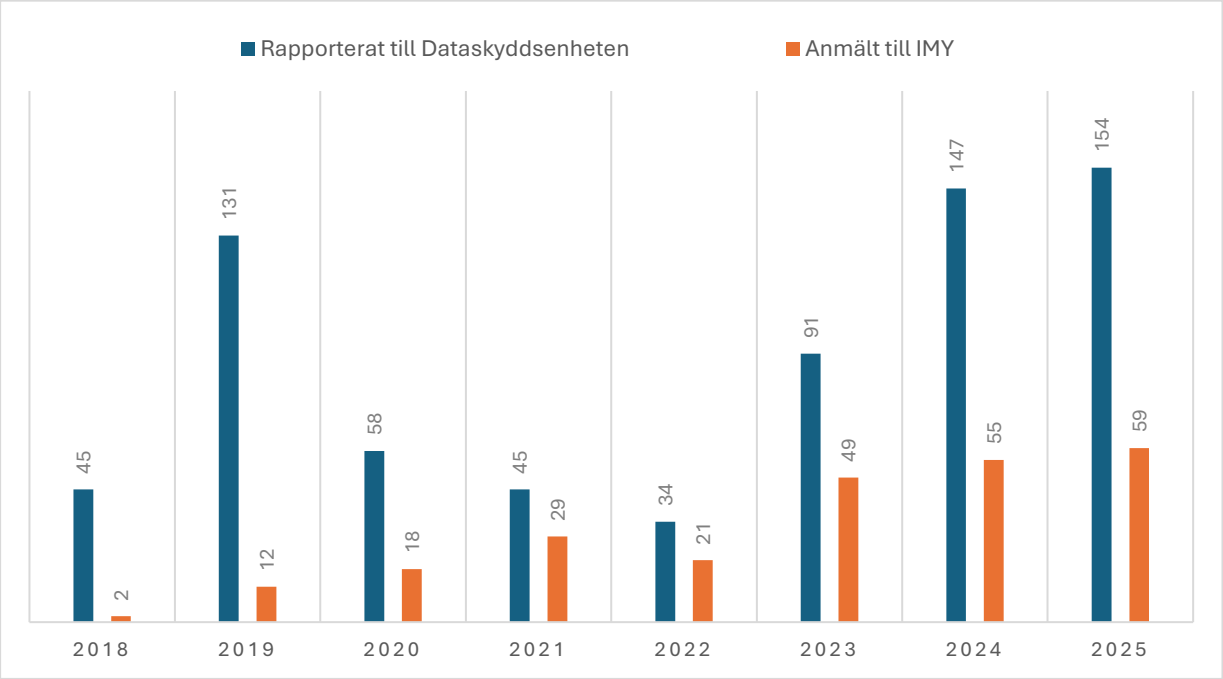
Under 2025 har 154 personuppgiftsincidenter rapporterats, där regionen har bedömts vara personuppgiftsansvarig. Av dessa bedömdes 59 incidenter kunna innebära risk för den registrerade varför de anmäldes till Integritetsskyddsmyndigheten (IMY). IMY har i samtliga fall valt att ej vidta åtgärd.

[1] Se dnr. RS250511

Nedan anges antal personuppgiftsincidenter rapporterade per personuppgiftsansvarig nämnd.

Driftnämnd Hallands sjukhus	69
Driftnämnd Kultur och skola	1
Ambulans, diagnostik och hälsa	13
Driftnämnd Kollektivtrafik	1
Driftnämnd Psykiatrin	23
Regionstyrelsen	7
Driftnämnd Närsjukvård	33
Driftnämnd Regionservice	8

Tabellen nedan visar antalet inrapporterade personuppgiftsincidenter under åren 2018 till 2025.



Dataskyddombudet har analyserat de rapporterade incidenterna och kan konstatera att 111 av 154 incidenter 2025 avser felskickade handlingar eller felregistrering av uppgifter. Flera av dessa kan antas bero på tidsbrist hos medarbetare som leder till misstag, men likt föregående år bedömer dataskyddsombudet att detta fynd även kan anses indikera ett behov av tydligare styrning och stöd avseende informationshantering inom regionen.

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 Hallandstrafiken

Under våren 2025 genomförde dataskyddsombudet en revision av Driftsnämnden för kollektivtrafiks efterlevnad av dataskyddsförordningen.[1] Kortfattat fann dataskyddsombudet en rad brister, bland annat ej uppdaterad registerförteckning och inga genomförda konsekvensbedömningar eller anmälda personuppgiftsincidenter. Med anledning av revisionen har dataskyddsombudet under 2025 utbildat samtliga anställda på förvaltningen (Hallandstrafiken) i dataskydd och dataskyddsombudet kan konstatera att förvaltningen har börjat vidta åtgärder efter revisionen, bland annat genom att inkomma med uppdaterad registerförteckning.

5.2 Säkerhetsprövning och bakgrundskontroller

Under hösten 2025 genomförde dataskyddsombudet en revision av Regionstyrelsens behandling av personuppgifter i samband med säkerhetsprövning och bakgrundskontroller.[2] Dataskyddsombudet fann bland annat behandlingen saknades i Region Hallands registerförteckning och att det saknades konsekvensbedömning trots att känsliga personuppgifter ofta behandlas i samband med denna process. Säkerhetsavdelningen, för Regionstyrelsens räkning, har sedan dess påbörjat arbetet med att vidta rekommenderade åtgärder.

5.3 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).

I slutet av 2025 påbörjade nuvarande dataskyddsombud en uppföljande revision, vilken färdigställdes i början på 2026.[3] Då ny kamerabevakningslagstiftning trädde i kraft 1 april 2025 utgick revisionen från den ny lagstiftningen.

Sammanfattningsvis kunde dataskyddsombudet konstatera att flertalet uppmärksammade brister från föregående revision inte hade åtgärdats, vilket innebär att dessa nämnder fortsatt bedriver olovlig kamerabevakning. Utifrån de nya reglerna i kamerabevakningslagen kunde det konstateras att majoriteten av nämnderna saknar fullgod dokumentation kopplat till pågående kamerabevakning. Vidare konstaterades Säkerhetsavdelningen, för Regionstyrelsens räkning, ha brustit i sitt samordningsansvar på området med anledning av att de inte har tillsett att adekvat styrning och samordning (genom styr- och stöddokumentation) finns inom regionen.

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. För att avgöra om en planerad personuppgiftsbehandling kräver konsekvensbedömning görs en så kallad förhandsbedömning.

Under 2025 har 9 förhandsbedömningar, med bedömningen att konsekvensbedömning inte är nödvändig, genomförts. 12 kompletta konsekvensbedömningar har genomförts.

[1] Se dnr. RS250578
[2] Se dnr. RS251707
[3] Se dnr. RS260264

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 informationssäkerhets- och dataskyddsfunktionerna och till regionens olika verksamheter under året. Dataskyddsombudet har också handlagt ett antal frågor, lämnat rekommendationer på genomförda konsekvensbedömningar, samt genomfört flertalet utbildningar för olika delar av regionens verksamhet. Bland annat har samtliga anställda inom Hallandstrafikens verksamhet fått grundläggande utbildning i GDPR under 2025.

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 registerutdrag. 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 2025 inga klagomål eller begäran om att utöva sina rättigheter inkommit till dataskyddsombudet. Till dataskyddsfunktionen har 3 begäran om registerutdrag inkommit, vilka har hanterats inom en månad från inkommandet. Inga klagomål har inkommit till funktionen.

9 Omvärldsbevakning

NIS2, EU-direktivet för höjd cybersäkerhet, trädde i kraft i svensk lagstiftning den 15 januari 2026 genom cybersäkerhetslagen. Den nya lagstiftningen har påverkat informationssäkerhetsfunktionen i stor grad under 2025 på grund av deras arbete med att säkerställa att regionen är redo att omhänderta de nya krav som uppkom i samband med ikraftträdandet. Detta arbete fortgår även under 2026. Kopplat till informationssäkerhet- och dataskyddsområdet måste AI-förordningen, som delvis trädde i kraft den 1 augusti 2024, också nämnas. De flesta bestämmelser i denna förordning träder i kraft den 2 augusti 2026, och medför stora krav på dokumentation och riskbedömningar vid införande av AI-lösningar. Dessa processer och nya formkrav kommer behöva samverka med befintliga dataskyddsprocesser. Utifrån den information dataskyddsombudet har fått från Regionkontoret kan det konstateras att regionen ännu inte har tillsett att ansvar, resurser och kompetens för denna hantering är säkrad, vilket enligt dataskyddsombudets bedömning medför stor risk att regionen inte kommer vara redo att omhänderta de nya kraven i augusti 2026.

10 Dataskyddsombudets mål för 2026

Dataskyddsombudet planerar att under H1 2026 fokusera på att stötta Säkerhetsavdelningen i framtagandet av samordning och styrning kopplat till kamerabevakning, samt stötta dataskyddsfunktionen i revisionsarbetet av ledningssystemet. Under H2 planerar dataskyddsombudet att genomföra en-två revisioner i enlighet med tillsynsplan.

Dataskyddsombudet tackar alla i regionen för ett gott samarbete under 2025 och hoppas på ett fortsatt gott samarbete under 2026.

Ellen Bäckman, dataskyddsombud