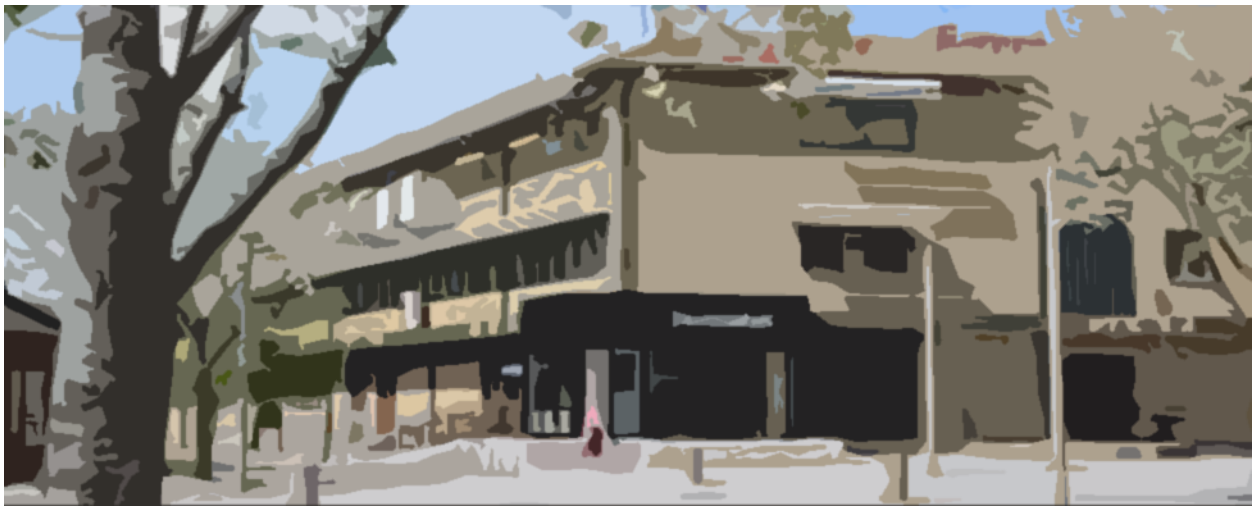

ÅRSRAPPORT DATASKYDD 2024 SAMT RESULTAT FRÅN GRANSKNING AV BEHANDLINGSREGISTREN

Den här rapporten handlar om dataskyddsombudets arbete och samlade iakttagelser av arbetet med data- och integritetsskyddet i Hylte kommun under 2024. I denna rapport redogörs även för resultat från granskning av behandlingsregistren. Målgrupp är främst de personuppgiftsansvariga nämnderna och styrelserna inom kommunen men även de som aktivt arbetar med frågorna eller berörs av området i sitt arbete.

Jessica Karlsson, dataskyddsombud för kommunerna Falkenberg, Laholm och Hylte
2025-07-07

INNEHÅLLSFÖRTECKNING

Sammanfattning

Den här rapporten handlar om dataskyddsombudets arbete och samlade iakttagelser av arbetet med data- och integritetsskyddet i Hylte kommun under 2024. I rapporten finns också ett avsnitt med redogörelse för resultat av den granskning som gjorts av behandlingsregistren. Målgrupp för denna rapport är främst de personuppgiftsansvariga nämnderna och styrelserna inom kommunen men även de som aktivt arbetar med frågorna eller som på något sätt berörs av området i sitt arbete. Rapporten omfattar följande personuppgiftsansvariga i Hylte kommun; kommunstyrelsen, tillsynsnämnden, barn- och ungdomsnämnden, samhällsbyggnadsnämnden, kultur- och folkhälsonämnden, omsorgsnämnden samt Stiftelsen Hyltebostäder.

Ett generellt råd till samtliga personuppgiftsansvariga är att i högre grad lyfta in och integrera dataskyddet i lednings- och utvecklingsfrågorna och att aktivt resursfördela och följa upp arbetet.

Om dataskyddsombudet ska peka på några mer specifika områden där det finns utvecklingspotential, så är det området tröskelanalyser och risk- och konsekvensbedömningar, DPIA. Arbetet med DPIA ska göras innan en behandling påbörjas av personuppgifter och/eller innan en upphandling av exempelvis ett nytt IT-system påbörjas. Och det för att dels säkerställa att det man tänker göra med person-uppgifterna är lagligt, lämpligt och nödvändigt. Bedömningen bidrar dels också med underlag till krav som behöver ställas på en leverantör av ett system vad gäller till exempel säkerhetsnivån i systemet och hos leverantören. Dataskyddsombudet bedömer att alldeles för få tröskelanalyser och DPIA görs i Hylte kommun sett i relation till den stora mängd personuppgifter som hanteras och den verksamhetsutveckling/digitalisering som pågår.

Verksamheterna behöver också skaffa sig en djupare kunskap om vad som räknas som personuppgifter (något som framkom tydligt i granskningen av behandlingsregistren). Med personuppgift avses varje upplysning som avser en identifierad eller identifierbar fysisk person. Avgörande är att uppgiften, enskilt eller i kombination med andra uppgifter, direkt eller indirekt, kan knytas till en levande person.

Vidare måste verksamheterna bli bättre insatta i vad en personuppgiftsincident är för något och att de ska anmälas, utredas och dokumenteras enligt interna rutiner. Ibland ska de även anmälas till IMY, Integritetsskyddsmyndigheten.

Dataskyddsombudet rekommenderar respektive verksamhets personuppgiftssamordnare att regel-bundet delta vid ledningsgrupper, nämnder/styrelser, APT, utvecklingsprojekt osv för att informera och utbilda inom området dataskydd och vad regelverket ställer för krav på verksamheternas person-uppgiftshantering.

Granskningen av behandlingsregistren visar på betydande brister. Det finns finns ett omfattande arbete att göra för verksamheterna för att leva upp till kraven på ett behandlingsregister enligt artikel 30 i GDPR. De flesta av behandlingarna har man inte sett över sedan de gjordes runt åren 2018 – 2019, dvs i samband med att den nya dataskyddslagstiftningen infördes. Ändamålen som anges i de register som

granskats är i många fall otydliga, abstrakta och ospecifika samt att den direkta kopplingen till varför personuppgifter behandlas inte går att förstå.

Vidare har verksamheterna svårt att avgöra vilken rättslig grund som gäller för att få behandla personuppgifter. Alltför ofta anger man samtycke som laglig grund. Denna grund är som regel inte tillämpbar inom offentlig verksamhet. Beroende på vilken rättslig grund som åberopas enligt GDPR så krävs ofta också att man anger vilket nationellt lagstöd man grundat sin behandling i.

Angivelse av tidsfrister för radering av personuppgifter saknas bitvis, det saknas uppgifter om biträden och om biträdesavtal är tecknade samt om det sker någon tredjelandsöverföring av personuppgifter.

Att förstå och tillämpa de olika leden i GDPRs artikel 30.1 om behandlingsregister är inte så enkelt som det kan uppfattas vid en första anblick och det är något som blivit tydligt i samband med genomförd granskning. Kunskapen om regelverket och hur praktiskt arbeta med behandlingsregistren är högre idag än 2018-2019 då behandlingarna förtecknades. Förutsättningarna för arbetet utifrån den aspekten bör därför vara bättre idag. Men då måste verksamheterna avsätta resurser i form av tid och personer som kan arbeta med behandlingsregistren. Ett komplett behandlingsregister bidrar till att kommunen får ett bättre stöd i det fortsatta arbetet med dataskydd. Intensifieras dessutom arbetet med risk- och konsekvensbedömningar så bidrar det också med information till behandlingsregister och biträdesavtal.

1. Syftet med årsrapporten och granskningen

Syftet med den här rapporten, förutom att den också ger en bild av dataskyddsombudets arbete och insatser under året, är att underlätta för både kommunstyrelsen och de olika personuppgiftsansvariga nämnderna och styrelserna inom kommunen att följa upp och göra rätt prioriteringar för att stärka data- och integritetsskyddet framöver. Utöver det egenkontrollarbete som varje personuppgiftsansvarig själv behöver genomföra för sin verksamhet, blir årsrapporten ett sätt att få en oberoende blick på kommunens status på dataskyddsarbetet och de utvecklingsbehov som kan finnas på området.

I rapporten finns också ett avsnitt med redogörelse för resultatet av den granskning som gjorts av behandlingsregistren vilket också kommer bidra med stöd till kommunens fortsatta arbete med dataskydd.

Rapporten, inklusive granskningen, omfattar följande personuppgiftsansvariga i Hylte kommun; kommunstyrelsen, tillsynsnämnden, barn- och ungdomsnämnden, samhällsbyggnadsnämnden, kultur- och folkhälsonämnden, omsorgsnämnden samt Stiftelsen Hyltebostäder.

1.1 Dataskyddsombudets roll

Uppdraget som dataskyddsombud är fastställt i GDPR (Allmänna dataskyddsförordningen/General Data Protection Regulation, Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG). Där står att dataskyddsombudet (DSO) självständigt och oberoende ska följa och granska personuppgiftshanteringen i förhållande till bestämmelserna i GDPR för de verksamheter som DSO är utsedd att vara ombud för. Där står också att DSO ska rapportera iakttagelser till den högsta ledningen, så att den som ytterst ansvarar för verksamheten (den personuppgiftsansvarige) kan vidta åtgärder för att stärka data- och integritets-skyddet. DSO-uppdraget omfattar även att ge råd och stöd till medarbetare och chefer i den operativa verksamheten, exempelvis genom information eller råd vid särskilt riskfylld hantering av person-uppgifter. Utöver GDPR och angränsande bestämmelser som ram för uppdraget, så är utgångspunkten alltid de registrerades perspektiv.

Dataskyddsombudet för Hylte kommun är även ombud för kommunerna Laholm och Falkenberg. Det innebär att dataskyddsombudet bistår och granskar totalt 35 styrelser och nämnder (bolag inkluderat).

1.2 En fråga om trygghet

Dataskydd är ett begrepp för allt det som gör att människors personuppgifter är i trygga händer när de samlas in, bearbetas, delas, lagras eller hanteras på annat sätt. Det handlar om allt från att ha ordning och reda med hjälp av rutiner av olika slag som exempelvis beredskap att hantera risker till att sätta

upp tekniska skyddsåtgärder i system och digitala verktyg och att se till att personalen genom sin uppmärksamhet och kunskap bidrar till att upprätthålla dataskyddet. Både i det dagliga arbetet och när verksamheten utvecklas.

Skyddet är omfattande och regleras av EU-förordningen GDPR, kompletterat med den svenska dataskyddslagen och en rad andra bestämmelser inom olika verksamhetsområden. Dataskydd kan därför uppfattas som regeltungt, men också tekniskt och abstrakt eftersom det många gånger handlar om flöden av personuppgifter ”i kulisserna” till de tekniska verktyg vi använder.

Men data- och integritetsskyddsfrågor ska först och främst ses som en trygghetsfråga för dem vars personuppgifter kommunen hanterar. Frågan har kommit att bli högaktuell i och med den intensiva innovativa och datadrivna teknikutvecklingen som sker i samhället. Omfattningen av personuppgifter som hanteras har aldrig varit så stor som den är idag och mot bakgrund av hoten i vår omvärld har den personliga integriteten därför heller aldrig varit viktigare att värna.

För att det ska vara hållbart att använda digitaliseringens möjligheter och dra nytta av den nya tekniken, med syftet en bibehållen välfärd och demokrati, måste det alltså göras på integritetsvänliga sätt. Dataskyddsperspektivet måste därför finnas med när nya arbetssätt utvecklas så att vi kan lita på de digitala tjänster som används och utvecklas. Dataskyddsarbetet måste ingå som en självklar del när nya digitala lösningar för människor tas fram. Inbyggt dataskydd och dataskydd som standard är centrala begrepp som vid tjänste-/systemdesign måste få en självklar påverkan på de system och tjänster som används.

Utgångspunkten i GDPR är att individens rätt till integritet och skydd för sina personuppgifter är viktigare än en organisations behov av att samla in, bearbeta och dela personuppgifter hur som helst. Den grundlagsskyddade rätten till integritet är många gånger också ett led i att tillvarata andra fri- och rättigheter. Till exempel rörelsefriheten – att inte bli övervakad, rätten att fritt bilda åsikter och rätten att inte bli diskriminerad. Det är i det ljuset som GDPR har kommit till. För utan GDPR vore det mer ”fritt fram” att använda våra personuppgifter för sådant som profilering, åsiktsregistrering, förföljelse och utestängning samt aktioner för att felaktigt påverka våra uppfattningar och vår tillit till samhället. Möjligheterna att följa, kartlägga och påverka människor ökar exponentiellt med den nya tekniken. Information om sjukdomar, funktionsnedsättningar, beteenden, facklig tillhörighet eller andra integritetskänsliga uppgifter kan få förödande konsekvenser för enskilda om informationen kommer i fel händer. Eller om det politiska läget förändras. Med den digitala tekniken och de datamängder som den genererar om oss människor och våra beteenden blir uppgifter om oss och våra preferenser mer tillgängliga att använda av olika aktörer för olika ändamål. Det är här GDPR kommer in och sätter ramarna så att tekniken inte ska leda till en insamling och användning av personuppgifter som riskerar att äventyra människors grundläggande fri- och rättigheter i ett demokratiskt samhälle.

1.3 Kommunen har en särskild roll

Kommunen har med sin särställning, såsom värnare av sina invånares intressen och demokratin, ett extra ansvar att måna om ett gott integritets- och dataskydd i sin service och sina åtaganden. Alla ansträngningar som görs kopplat till dataskyddet i kommunen tjänar därför ett högre syfte än ”bara” regelefterlevnad och teknisk administrering. Dataskydd handlar främst om människor.

2. Dataskyddsombudets råd och stöd

2.1 Information och utbildning

Dataskyddsombudet är stående **deltagare på Hylte kommuns nätverk för personuppgifts-samordnare** (PUS) vilket drivs av kommunens informationssäkerhetssamordnare. Syftet med nätverket är att underlätta för verksamheterna och skapa samsyn i arbetet med dataskydd. Syftet är också att i ett gemensamt forum diskutera diverse frågor kopplat till verksamheternas personuppgifts-hantering, skapa rutiner för arbetet, omvärldsbevaka, lära av varandra mm för att få ett så effektivt arbete som möjligt kring dataskyddsfrågorna och på ett kommunövergripande plan. Inriktningen av nätverket går också emot att även täcka frågor inom hela informationssäkerhetsområdet. PUSarna arbetar enligt ett fastställt årshjul som bidrar till att sätta agendan för vad som avhandlas vid dessa nätverksträffar. Nätverket har haft fem möten under året och består av deltagare som arbetar med dataskydd och som även delvis påbörjat arbetet inom informationssäkerhetsområdet. Nätverket bestod 2024 av femton (15) personer/personuppgiftssamordnare och representerade kommunens samtliga nämnder och styrelser.

På nätverksträffarna har dataskyddsombudet en stående informationspunkt. Informationen består av omvärldsbevakning; vad är på gång inom dataskyddsarbetet i de tre kommunerna som dataskydds-ombudet arbetar för, nya rättsfall och beslut från domstolar, Integritetsmyndigheten (IMY) och EU samt specifik information i något ämne som är särskilt aktuellt eller ren utbildning.

Alla kommunens personuppgiftsansvariga, dvs alla nämnder och styrelser, har under året fått besök av dataskyddsombudet tillsammans med kommunens informationssäkerhetssamordnare. Information gavs om värdet av att arbeta med dataskydd utifrån GDPR, risker för dataintrång som kan innebära stöld av information och personuppgifter och hur viktigt det är att prioritera informations-säkerhet bl. a vid införande av ny teknik. Det gavs även information om själva regelverket rörande personuppgifter och informationssäkerhet, om ansvar, roller och hur arbetet med dataskydd bedrivs inom kommunen.

Dataskyddsombudet har dessutom **regelbundna avstämningar med kanslicheferna i Laholm, Falkenberg och Hylte** angående arbetet med dataskydd som till exempel aktuella risk- och konsekvensbedömningar, diverse ärenden, omvärldsbevakning, arbetsbelastning osv.

2.2 Råd och rekommendationer

2.2.1 Risk- och konsekvensbedömningar, DPIA

De som är personuppgiftsansvariga för en kommande/pågående personuppgiftsbehandling måste säkerställa och visa att behandlingen följer GDPR.

Av artikel 35.1 i GDPR följer; ”Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter” dvs. en risk- och konsekvensbedömning, en s.k. DPIA (Data Protection Impact Assessment). För att kunna avgöra om det krävs en DPIA inför en behandling av personuppgifter utförs först en s.k. tröskelanalys. Den kan då resultera i att man inte behöver gå vidare med en DPIA. Men i de flesta fall resulterar den i att en DPIA måste göras.

Den som är personuppgiftsansvarig är skyldig att fråga sitt dataskyddsombud om råd i samband med konsekvensbedömningar. Dataskyddsombudet är i sin tur också skyldig att ge råd. Under året har dataskyddsombudet bistått verksamheterna i deras arbete med dessa och dessutom lämnat yttranden med synpunkter och råd inför behandlingarna. Under 2024 inkom fyra (4) konsekvensbedömningar till dataskyddsombudet. Nedan finns en översikt över dessa.

Tabell 1. Hylte kommuns gjorda risk- och konsekvensbedömningar (DPIA) under 2024

Nämnd/styrelse	Behandling	Kommentar
Samhällsbyggnadsnämnden DPIA	Behandling av personuppgifter i samband med administration av renhållnings- och avfallshanterings-processen, nytt system EDP Mobile	I systemet ingår positioneringsteknik vilket möjliggör en närgången övervakning av anställda och medför risker för otillbörliga integritetsintrång
Samhällsbyggnadsnämnden DPIA	Digital felanmälan gata- och park	Positionsangivelse möjlig. Det finns även risk för onödig spridning av personuppgifter

Samhällsbyggnadsnämnden DPIA	Digitalt språkverktyg för att stärka utrikesföddas språkkunskaper, Lingio	Känsliga uppgifter i form av etnicitet. Även i övrigt integritetskänsliga uppgifter behandlas - som värderande information som omdömen/betyg/ resultat.
Kultur- och folkhälsonämnden DPIA	Administrations- och informations-verktyg för verksamhet på fritidsgårdar, Ungdomsappen	Uppgifter om barn är extra skyddsvärda. Behandling av känsliga personuppgifter utan laglig grund, risk för profilering, leverantör behandlar kommunens personuppgifter för egna syften samt ev. tredjelandsöverföring av personuppgifter.

Med tanke på den omfattande verksamhet som kommunen inklusive Hyltebostäder bedriver och den utveckling som sker genom digitalisering av diverse processer, i vilka personuppgifter oftast förekommer, borde det totala antalet tröskelanalyser och DPIA varit betydligt högre. Det är därför viktigt att kommunen verkar för att få in tröskelanalyser och DPIA i befintliga processer inför utveckling och upphandling av nya IT-system och tjänster.

2.2.2 Biträdesrelationer och avtal

Som en följd av att nya system och tjänster upphandlas, så uppstår oftast behov av att **teckna biträdesavtal** i de fall externa parter är involverade i hanteringen av kommunens data på något sätt. Dataskyddsombudet ger ofta råd i ärenden om biträdesavtal - om sådana behövs eller inte, vem som är personuppgiftsansvarig, vem som är biträde och vilka som är underbiträden. Frågor kopplat till detta område landar många gånger i att en mindre utredning måste göras. I den försöker man kartlägga vem som är ansvarig för vad, vem bestämmer ändamål och medel för behandlingen av personuppgifter, hur ser flödena av information/ personuppgifter ut mellan berörda parter osv. Antal ärenden om biträdesavtal som dataskyddsombudet bistått i var tre (3) under 2024.

2.2.3 Personuppgiftsincidenter

Ett annat område jag som dataskyddsombud involveras i är råd och stöd, om verksamheterna vill och behöver det, vid misstänkta **personuppgiftsincidenter**. Även registrerade, tex kommuninvånare, kan kontakta mig direkt vid misstanke om incidenter som tex. dataintrång. Incidenter är händelser där enskilda riskerar att drabbas av negativa konsekvenser på grund av att deras personuppgifter inte hanterats korrekt eller inte skyddats tillräckligt. Dessa händelser är verksamheterna skyldiga att uppmärksamma och hantera. Allvarliga incidenter ska dessutom med kort varsel (inom 72 timmar) rapporteras till Integritetsskydds-myndigheten (IMY).

Under året har jag bistått med hjälp kring hantering av två (2) incidenter. I ett fall handlade det om att en system- och tjänsteleverantör drabbats av en hackerattack och i det andra fallet hade en underleverantör gjort en leverans av läkemedel/medicinska hjälpmedel till fel person. Totala antalet anmälda incidenter i kommunen 2024 endast dessa två.

Att en verksamhet uppmärksammar och hanterar incidenter är i sig ett tecken på att verksamheten har personal som är vaksam och att det finns beredskap för att ta hand om den här typen av händelser. Det innebär en stor trygghet för de registrerade. Rapporterade och hanterade incidenter från verksamheten är alltså tecken på ett fungerande dataskydd, medan inga/knappt några incidenter i en verksamhet som hanterar stora mängder personuppgifter väcker frågor – även om det finns rutiner. Varje hanterad incident leder till att dataskyddet stärks – både i den enskilda situationen och på en övergripande nivå, eftersom åtgärder vidtas för att förebygga att liknande händelser upprepas. Därför är det viktigt att verksamheterna regelbundet analyserar sin incidenthantering. Grunden till en fungerande rapportering av incidenter är att göra begreppet incident känd och även kommunicera hur incidenter ska hanteras inom organisationen. En tydlig och kontinuerlig information om detta kan ges via intranät, på APT och diverse verksamhetsmöten.

Skälen till att personuppgiftsincidenter uppstår är oftast den mänskliga faktorn. Orsaken kan nog många gånger handla om tidsbrist eller brist på uppmärksamhet när man handskats med personuppgifter, vilket exempelvis kan leda till att information skickas till fel mottagare. Samtidigt fortsätter den här typen av incidenter att förekomma även för verksamheter som har större vana och rutin på att uppmärksamma och hantera incidenter. Det tyder på ett behov av att jobba ännu mer med att stärka det tekniska skyddet så att utrymmet för att göra mänskliga misstag minskar. Det handlar också om att fortsätta vidareutbilda personal samt identifiera de organisatoriska situationerna där misstag uppstår.

Många incidenter kan sägas uppstå utanför verksamheternas kontroll och då genom att externa parter som leverantörer av IT-system och IT-tjänster drabbas av hackerattacker eller att de gör uppdateringar av systemen som inte är riktigt genomtänkta och data går förlorad eller läcker ut. När det handlar om externa parter så utgör de ofta biträden till kommunen i hanteringen av personuppgifter. Det krävs att kommunen redan inför en upphandling av ett system ställer krav på informationssäkerhet och GDPR efterlevnad av blivande leverantörer eftersom kommunen blir ytterst ansvarig i egenskap av personuppgiftsansvarig för den hantering som biträdet gör åt kommunen. Det är oerhört viktigt att det i avtal och i biträdesavtal som tecknas framgår vilka krav kommunen har på informationssäkerhet och personuppgiftshantering.

2.2.4 Råd om tredjelandsöverföring och AI-användning

Dataskyddsombudet såg under 2024 ett behov av att göra ett förtydligande kring vad som gäller kring tredjelandsöverföring av personuppgifter. Det resulterade i ett PM; **”Information och råd - överföring av personuppgifter till tredje land”**. Det innehåller ett antal råd som DSO rekommenderar verksamheterna att beakta inför eventuella tredjelandsöverföringar generellt men i synnerhet överföringar till USA och det eftersom det är det vanligaste tredjelandet dit överföring sker eller riskerar att ske till.

Dataskyddsombuden i Halland fick fler och fler signaler under 2024 på att AI-användningen börjat ta fart i kommunerna. Ett akut behov fanns därmed av att ta fram någon form av vägledning avseende användning av AI-teknik**.** Ombuden arbetade därför tillsammans fram väg-ledningen ”**Dataskyddsombudens råd inför användning av AI”**. Den har skickats ut till alla kommunerna (samtliga PUA - nämnder och styrelser) i Hallands län. Vägledningen består av sju råd om de områden som dataskyddsombuden i Halland ser som särskilt kritiska för att kommunen ska kunna förena sin användning av AI med ett tryggt dataskydd;

1. Använd GDPR som möjliggörare
2. Förstå konsekvenserna och tekniken
3. Ha koll och kontroll
4. Använd etablerade resurser
5. Hantera AI-riskerna
6. Använd oberoende experter
7. Använd integritetsvänlig teknik

Målgruppen för råden är alla som planerar att använda AI, men främst de som arbetar med utveckling och införande av arbetsprocesser där AI kan komma att ingå som verktyg samt ansvariga för verksamheten och de ytterst personuppgiftsansvariga dvs nämnder och styrelser.

2.3 Diverse ärenden/frågor

Dataskyddsombudet har under året även bistått i fem (5) övriga **ärenden** som rört frågor kring regelverket och det praktiska arbetet kring personuppgiftshantering. Frågorna kom från medarbetare inom kommunen. Inga frågor/ärenden har under 2024 inkommit direkt från någon registrerad till dataskyddsombudet.

Dataskyddsombudet har även deltagit vid några möten med ATEA och Microsoft som bl. a IT-enheten och informationssäkerhetsamordnaren haft inför kommunens **planerade införande** av **M365**. Dataskydds-ombudet har inför dessa träffar gått igenom en hel del material.

3. Samverkan

Dataskyddsombudet har ett nära och bra samarbete med Hylte kommuns **informationssäkerhetssamordnare**. Kommunens informationssäkerhetssamordnare har i sin tur regelbunden kontakt med personuppgiftssamordnarna och bistår dem med hjälp och stöd på olika sätt. Även dataskyddsombudet kan ha direktkontakt med personuppgiftssamordnarna. DSOs bild är att informationssäkerhetssamordnaren drar ett stort lass i arbetet med dataskydd i kommunen. Flera av de personuppgiftsansvariga nämnderna/styrelserna behöver verka för att själva ta ett större ansvar för arbetet med dataskydd. Det är ju dessutom de personuppgiftsansvariga med sina verksamheter som själva har bäst kunskap om vilka personuppgifter man hanterar i vilka sammanhang och varför och som ska säkerställa att GDPRs krav efterföljs. Viljan till och behovet av digitalisering och nya lösningar upplever DSO som hög i Hylte kommun. Därmed kommer kommunens hantering av personuppgifter och information att öka. Och med tanke på de ökande hoten i vår omvärld i form av cyberattacker mot företag och myndigheter, marknadens enorma flora av diverse digitala verktyg och tjänster, än mer avancerade verktyg med komplexa inslag som AI-teknik så blir behovet av att värna den personliga integriteten större än någonsin och därmed också behovet av ytterligare resurser i arbetet med dataskydd. Det kommer dessutom mängder med nya krav på myndigheter och organisationer i form av ny lagstiftning som NIS2, AI-Act mm. Kommunledningen behöver därför säkra upp med resurser i form av **fler medarbetare som ges utökat utrymme att arbeta med frågorna**, tillse att det är ”rätt person på rätt plats” vad gäller detta arbete samt satsa på **utbildning inom den nya tekniken och regelverket**.

En gång per månad träffas **samtliga dataskyddsombud för Hallands kommuner och Region Halland**. Antalet ombud är i nuläget sex. Det är en värdefull samverkan där det diskuteras aktuella frågor och ärenden från kommunerna och omvärlden. Frågor som diskuterats under 2024 har bland annat rört personuppgiftsansvar, rättsliga grunder och användning av AI-teknik. DSOerna i Halland var även värdar för det stora nätverket ”DSO i Väst” i november 2024. Temat var AI och dataskydd samt samverkan med IMY. Värdskapet innebar en hel del arbete i form av planering, ta fram dagordning, hålla föredrag och leda diskussioner.

Nätverket ”**DSO i Väst**” består av ca ett trettiotal dataskyddsombud i kommuner och regioner i västra Sverige. Nätverket har funnits sedan år 2018. I nätverket finns både DSOer som är anställda direkt vid kommunerna och regionerna och DSOer som arbetar via kommunalförbund eller privata företag. Tillsammans bistår och granskar vi ca 400 personuppgiftsansvariga vars verksamheter berör ca 2 miljoner registrerade, om inte fler. Vi träffas en gång i halvåret för att diskutera gemensamma frågeställningar och lära av varandra.

Under 2024 initierade nätverket DSO i Väst en möjlighet till **samverkan med IMY**. Undertecknad tillsammans med fem andra ombud bildade en arbetsgrupp för att ta fram förslag på samverkansområden. Förslaget skickades till IMY och de ställde sig positiva till samverkan och då kring ett av våra förslag som handlade om behovet av att ta fram en vägledning för arbete med behandlingsregister. Arbetsgruppen bjöds in till IMY i Stockholm för diskussion kring samverkan. Dock resulterade det inte i att en samverkan inleddes. De angav att de hade andra prioriteringar framöver än det förslag om behandlingsregister som vi

hade enats kring. Arbetsgruppen har dock bestämt sig för att nätverket i väst själva arbetar fram en vägledning för behandlingsregister utan samverkan med IMY.

Dataskyddsombudet är också **medlem i Forum för Dataskydd** (DP-Forum). Forumet arbetar för att stärka dataskyddsombud och andra som arbetar med eller kommer i kontakt med dataskyddsfrågor. Vidare lämnar de synpunkter på lagförslag, kommenterar aktuella frågor i media och föreläser vid diverse lärosäten. Forumet arrangerar löpande webbinarier, utbildningar, konferenser samt nätverksträffar för sina medlemmar men även för icke medlemmar.

Dataskyddsombudets **kontakt med IMY** har under året har främst bestått i nyttjandet av dess upplysningstjänst, deltagande vid den årliga konferensen som myndigheten anordnar för dataskydds-ombud, ett antal webbinarier med olika teman samt det ovan nämnda försöket till samverkan. Inga kontakter har föranletts på grund av något ärende i kommunen som tillsyn eller klagomål.

4. Kommande år

Grundläggande för ett funktionellt dataskydd är att den personuppgiftsansvarige, dvs respektive nämnd och styrelse, har koll på sin behandling och då på vilka personuppgifter som behandlas och på allt det som görs med dem inom det egna ansvarsområdet. Detta ska deklareras i ett register, ett så kallat **behandlings-register**, enligt artikel 30 i GDPR. Registret får inte vara utformat hur som helst utan det ska vara lätt att utläsa vad behandlingen består i utifrån de krav som GDPR ställer på registrets innehåll.

Om det finns betydande brister i registret är det svårt att bedriva ett bra arbete med dataskydd. Ett komplett och korrekt register utgör grunden för ett framgångsrikt GDPR-arbete. Utifrån att DSO gjort en snabb inventering av registren i de tre kommunerna så framkom att registren inte är kompletta i dagsläget. Därav bedömdes det lämpligt att genomföra en granskning av dessa.

Granskningen av behandlingsregistren i Hylte är avslutad och resultaten ifrån den presenteras under avsnitt fem (5) i denna rapport. I kommunernas verksamhet är det oftast personuppgiftssamordnaren, pus, för varje nämnd/styrelse som samordnar att registret upprättas alternativt att pus upprättar registret själv. DSO konstaterade brister i registren och rekommenderar därför verksamheterna att under resterande delen av året fokusera på arbetet med dessa.

I övrigt kommer ombudet ha **fortsatt fokus på tredjelandsöverföring och då i synnerhet på överföringar till USA.** Det pga. att den nya presidenten och hans administration påbörjat en översyn av tidigare beslut (presidentordrar) tagna av president Biden vilka rör nationell säkerhet. EU-US Data Privacy Framework beslutades av EU-kommissionen år 2023 och det för att återigen möjliggöra överföring av personuppgifter till mottagare i USA, särskilt leverantörer av molntjänster och det efter att Privacy Shield, som tidigare utgjort möjlighet att överföra personuppgifter till USA, ogiltigförklarats år 2020 genom Schrems II-målet. Leverantörer av populära molntjänster, däribland Microsoft, Google och Amazon, använder idag regelbundet EU-US Data Privacy Framework som rättslig grund för överföring av

personuppgifter till USA. Men då Trumps översyn även omfattar sådana presidentordrar som ligger till grund för EU-US Data Privacy Framework kan detta innebära slutet för ramverket, det finns alltså en risk för en Schrems III. Det leder återigen till att överföring till USA inte blir möjlig/laglig. Och det för att det kommer finnas möjlighet och ökad risk för att amerikanska myndigheter och underrättelsetjänster vidareutnyttjar personuppgifterna för sina egna ändamål och därmed utom kontroll för de personuppgiftsansvariga och de enskilda individerna.

Mot bakgrund av den snabba utvecklingen i omvärlden och ombudets iakttagelser i övrigt av kommunens verksamheter under det gångna året, så blir även ett annat specifikt riskområde särskilt väsentligt att följa och ha beredskap för att ge råd och stöd inom, och det är **integritetsskydd i samband med kommunens digitaliserings- och innovationsarbete där AI kommer vara en stor del**. Fokus blir därmed att ha beredskap för att uppmärksamma risker tidigt i arbetet så att kommunen inte bygger in integritetsfaror i sin strävan att dra nytta av nya tekniker och arbetssätt. Bedömningen är att efterfrågan på råd vid konsekvensbedömningar kommer att öka. Det är viktigt att berörda sätter sig in i alla nya regelverk bl. a AI-Act, som införs gradvis och ska vara helt införd under 2027.

Under hösten kommer DSOerna i Halland att hålla en **utbildning i hur man arbetar med risk- och konsekvensbedömningar, DPIA**. Målgruppen är samtliga kommuners dataskyddskontakter/personuppgiftssamordnare samt anställda som arbetar med digitalisering, utveckling och IT. Ombuden ser en möjlighet att bidra till att kommunerna drar nytta av dataskyddsarbetet, bl. a genom ökad kunskap om arbetet med DPIA, och det för att omställningsarbetet med att bli mer digital, innovativ och datadriven, ska bli integritetsvänligt och därmed hållbart för framtiden.

5. Resultat från granskning av behandlingsregistren

5.1 Syftet med granskningen

Grundläggande för ett funktionellt dataskydd är att den personuppgiftsansvarige, dvs respektive nämnd och styrelse, har koll på sin behandling och då på allt det som görs med personuppgifterna inom det egna ansvarsområdet. Detta ska deklareras i ett register, ett så kallat *behandlingsregister*, enligt artikel 30 i GDPR. Registret får inte vara utformat hur som helst utan det ska vara lätt att utläsa vad behandlingen består i utifrån de krav som GDPR ställer på registrets innehåll.

Behandlingsregistret är det sätt som den personuppgiftsansvarige deklarerar ändamål och medel för sin behandling samt ger information om vad som är okej att göra med personuppgifter i den aktuella verksamheten. Behandlingsregistret bör skötas av någon som är särskilt kunnig i dataskyddsfrågor och som kontinuerligt vakar över att de behandlingar som görs och förtecknas i registret är lagliga. I Hylte kommun är det oftast personuppgiftssamordnaren, pus, för varje nämnd som samordnar att registret upprättas alternativt att pus upprättar registret själv. Registret bör fastställas vid jämna mellanrum.

All personal som hanterar personuppgifter behöver veta vad de får behandla personuppgifter för och inom vilka ramar. Därför kan det vara bra att den ansvarige för registret regelbundet lämnar information om de

behandlingar som görs alternativt att registret är publicerat. Ett väl underhållet och tydligt beskrivet behandlingsregister underlättar också att ge korrekt och tydlig information till de registrerade.

En förutsättning för att påvisa efterlevnad av GDPR är att nämnden vet vilken information denne hanterar. Om det finns betydande brister i förteckningen är det svårt att bedriva ett bra arbete med dataskydd. Alla personuppgifter som hanteras av en nämnd eller styrelse måste vara kända för att kunna bli hanterade korrekt enligt GDPRs krav.

5.2 Metod för granskningen

I Hylte kommun använder man ett verktyg från leverantören Visma Draftit för upprättandet av behandlingsregister. Kommunens personuppgiftssamordnare och informationssäkerhetssamordnare arbetar i systemet. DSO har också tillgång till verktyget och har granskat behandlingarna genom att direkt i verktyget lämna synpunkter och kommentarer. En övergripande sammanfattning över granskningens resultat ges nedan.

Det totala antalet registrerade behandlingar för kommunen var ca trehundra (300) när DSO påbörjade granskningen i dec 2024. Antalet register med status ”klara för granskning” (en statusbenämning som den som är ansvarig för en behandling kan notera i verktyget) var då femtiofem (55). Det fanns tvåhundratrettionio (239) behandlingar status angiven till ” under bearbetning”. DSO tog inte hänsyn till angiven statusnivå vid sin granskning och granskade inte heller alla behandlingarna utan gjorde ett urval delvis baserat på en bedömning av vilka behandlingar som kan utgöra högriskbehandlingar men dels även utifrån annat i registret som av olika anledningar väckte ett intresse ur granskningssynpunkt. Totalt har DSO granskat lite mer än hälften av Hylte kommuns trehundra (300) behandlingar.

För barn- och ungdomsnämnden, BUN, landade det i att det i princip blev en totalgranskning av deras samtliga trettiosju (37) behandlingar. Anledningen till det, berodde på att den nämnden var den första som DSO började att granska och som DSO prövade olika arbetssätt på för granskningen. Med anledning av det har DSOs synpunkter på BUNs behandlingar till största delen lämnats över till BUN på listor utanför verktyget Draftit.

5.3 Resultat, rekommendation och avslutande kommentar

Respektive ansvarig för behandlingarna har direkt i verktyget fått återkoppling vid de avsnitt i registret där dataskyddsombudet bedömer att någon form av komplettering, revidering eller förtydligande behövs.

Under avsnitt 5.3.1 här i rapporten ges en sammanfattning av resultaten från granskningen samt slutsats och rekommendation.

5.3.1 Resultat och rekommendation

Det finns betydande brister i Hylte verksamheters dokumentation av behandlingar. Dataskyddsombudet bedömer att det finns ett omfattande arbete att göra för att leva upp till kraven i artikel 30 i GDPR. De flesta av behandlingarna har man inte sett över sedan de gjordes och det runt åren 2018 – 2019, dvs i samband

med att den nya dataskyddslagstiftningen infördes. Presentationen av resultaten görs nedan under ett antal områden utifrån vad ett behandlingsregister ska bestå av enligt GDPR.

Ändamålen med behandlingen
Enligt artikel 30.1b i GDPR ska behandlingsregistret innehålla ändamålen med behandlingen. Av GDPR:s grundläggande principer (artikel 5.1b i GDPR) framgår att personuppgifter endast får behandlas för särskilda, uttryckligt angivna och berättigade ändamål. Det betyder att uppgifterna måste vara adekvata och relevanta för ändamålen, och att de inte får vara mer omfattande än nödvändigt. Ändamålet med en behandling ska vara tydligt, konkret och specifikt. Med andra ord - den registrerade, dataskyddsombudet, eller tillsynsmyndigheten ska kunna läsa ändamålsbeskrivningen och, utan ytterligare kännedom om verksamheten, kunna förstå varför uppgifterna behöver samlas in och till vad de ska användas.

Ändamålen i de register som granskats är ofta otydliga och för kortfattade - beskrivningarna är ibland så kortfattade att det helt enkelt inte går att utläsa vad som avses och ibland kan man inte utläsa den direkta kopplingen till varför personuppgifter ens behandlas.

Många gånger likställer man ett helt system med en behandling, när man i stället ska ha fokus på varför och till vad en hantering av personuppgifter ska leda till - dvs vilket är ändamålet/syftet? Och därigenom visar det sig att ett system många gånger innehåller flera olika behandlingar med olika syften. I behandlingsregistren finns det därmed behandlingar som namnges med systemnamn (behandlingsregistren blir helt enkelt en systemförteckning) medan det i andra fall finns behandlingar som utgörs av ett enda dokument med personuppgifter vilket är en onödigt liten behandling att registrera. En sådan ”liten” behandling bör i stället kunna föras in i en mer övergripande/större behandling. I Hylte kommuns register över behandlingar finns det behandlingar som benämns nyckelskåp, brandsäkert arkivskåp, blanketter, pärm, Platina (systemets namn), känsliga personuppgifter, semesterlistor, scheman, beredskapslistor och liknande.

Många verksamheter har formulerat sina ändamål med utgångspunkt i vad man gör med uppgifterna och/eller hur man behandlar uppgifterna, dvs verksamhetens arbetsprocess. Detta missar dock målet eftersom ändamålet utgår ifrån varför personuppgifter behöver behandlas. I offentlig verksamhet har detta varför i många personuppgiftsbehandlingar sin grund i den lagstiftning som reglerar verksamheten. Så ett tips till verksamheterna är därför att utgå ifrån de lagkrav och de uppdrag som organisationen har att förhålla sig till och formulera sina ändamål utifrån dem. Det kanske inte alltid fungerar, men det är en bra utgångspunkt. Sen är det ju inte helt fel att ha sin utgångspunkt i arbetsprocesser som bedrivs, men glöm då inte bort att fokusera på målet med arbetsprocessen. Man kan även få lite ledning från dokumenthanteringsplaner/informationshanteringsplaner kring vilka personuppgifter som kan tänkas behandlas i verksamheterna och därefter undersöka vad ändamålet är. Och finns en systemförteckning, ja då kan det bidra med input till behandlingsregistret. Det handlar helt enkelt om att skaffa sig kunskap om verksamheten – vad gör man och vad ska det leda till.

Beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter
Något som dataskyddsombudet noterat är att man ofta missar vad som räknas som personuppgift. Med personuppgifter avses varje upplysning som avser en identifierad eller identifierbar fysisk person.

Avgörande är att uppgiften, enskilt eller i kombination med andra uppgifter, direkt eller indirekt, kan knytas till en levande person. Ett exempel - en faktura med medarbetares namn på kommer från företagshälsovården – i det fallet är det inte bara namnet som är en personuppgift. Att en medarbetare varit hos företagshälsovården indikerar att den anställde har problem med hälsan. Därmed behandlas ju ytterligare en personuppgift och som därmed ska anges i registret, ”uppgift om hälsa”, utöver uppgift om namn.

Enligt artikel 30.1c i GDPR ska behandlingsregistret innehålla en beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter. Det ska alltså framgå vilka uppgifterna är, vilka de registrerade (de vars personuppgifter man hanterar) är och hur de relaterar till varandra, det vill säga kopplingen mellan de registrerade och de uppgifter som behandlas.

Dataskyddsombudet kan konstatera att de granskade verksamheterna generellt har fyllt i kategorier av registrerade och kategorier av personuppgifter i behandlingsregistret. Men det beskrivs sällan vilka personuppgifter som behandlas för vilken kategori av registrerade (i de fall flera kategorier av registrerade anges). Vidare beskrivs kategori av registrerade ofta bristfälligt. I stället för att skriva ”anställda” så skulle verksamheten tex kunna skriva ”anställda handläggare som har till arbetsuppgift att handlägga ärenden om ekonomiskt bistånd” osv. Detsamma gäller för beskrivning av kategorierna av personuppgifter. Att enbart ange kategorier av personuppgifter som exempelvis ”kontaktuppgifter” ger inte svar på vilka personuppgifter som behandlas. Kontaktuppgifter ska därför beskrivas genom att exakt ange vilka dessa är, som namn, adress, e-post, telefonnummer osv.

Kategorier av mottagare
I artikel 30.1d i GDPR anges att behandlingsregistret ska innehålla uppgift om de kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, inklusive mottagare i tredjeländer eller i internationella organisationer. I artikel 4.9 i GDPR definieras begreppet mottagare. Mottagare kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas, vare sig det är en tredje part eller inte. Ett förtydligande av vad som avses med ”mottagare till vilka personuppgifterna lämnas ut” landar i att de man avser helt enkelt är den/de som har tillgång till/ges tillgång till uppgifterna på något sätt. Ett personuppgiftsbiträde är en mottagare, liksom underbiträden och under-underbiträde. Även de funktioner/roller som behandlar uppgifter inom en personuppgiftsansvarigs organisation/nämnd/förvaltning träffas av begreppet mottagare.

Dataskyddsombudet konstaterar att det finns brister i verksamheternas dokumentation av mottagare. I många fall saknas också uppgift om det finns personuppgiftsbiträden och då även i sådana fall där det är uppenbart att den behandling som beskrivs utförs med hjälp av personuppgiftsbiträden. Likaså saknas uppgift om det finns biträdesavtal.

Överföring av personuppgifter till tredjeland
Av artikel 30.1e i GDPR framgår att behandlingsregistret ska innehålla information om, i tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och, vid sådana överföringar som avses i artikel 49.1 andra stycket, dokumentation av lämpliga skyddsåtgärder.

Dataskyddsombudet noterar att verksamheterna ofta svarar vet ej på frågan om tredjelandsöverföring förekommer. Om det är så att någon del av behandlingen, hur ringa den än är, genomförs med hjälp av ett biträde eller underbiträde i tredje land, så ska den dokumenteras i behandlingsregistret – det vill säga vem/vilka biträden behandlar personuppgifter, varför och var.

Tidsfrister för radering
I artikel 30.1f i GDPR anges att den personuppgiftsansvarige ska, om det är möjligt, ange de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.

Efter att ha granskat verksamheternas behandlingsregister vill dataskyddsombudet särskilt förtydliga att artikel 30.1f föreskriver att det är tidsfristerna som ska anges. Det är inte tillräckligt att ange att gallringsbeslut finns, eller att det framgår av en dokumenthanteringsplan hur länge uppgifterna kommer sparas. Ett sådant förfarande uppfyller inte kravet om att ange tidsfrister i registret, utan informerar endast om att tidsfrister finns.

Allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder
Dataskyddsombudets samlade bedömning efter genomförd granskning av de utvalda verksamheterna är att beskrivningen av tekniska och organisatoriska säkerhetsåtgärder genomgående är bristfällig. I många fall saknas beskrivningen helt. Det är inte nödvändigt att återge alla rutiner eller åtgärder som tagits fram för att säkerställa korrekt behandling, utan bara de som hänför sig till behandlingens säkerhet i enlighet med kriterierna i artikel 32.1.

Rättslig grund och motivering
Dokumentation av en behandlings rättsliga grund, motivering av den rättsliga grunden och hänvisning till stödet för den rättsliga grunden i behandlingsregistret är inget krav enligt artikel 30 i GDPR. Den rättsliga grunden är dock själva förutsättningen för att lagligen få behandla personuppgifter och alla behandlingar måste stödjas på en av de rättsliga grunderna i GDPR. Utan en rättslig grund är behandlingen inte laglig. I Draftits verktyg finns laglig grund med som en obligatorisk punkt att besvara, vilket är mycket bra.

Dataskyddsombudet noterar i sin granskning att verksamheterna har svårt att avgöra vilken rättslig grund som gäller för att få utföra en behandling av personuppgifter. Alltför ofta anger man samtycke som laglig grund. Denna grund är som regel inte tillämpbar inom offentlig verksamhet och det har bl. a att göra med att de vars personuppgifter som hanteras, de står ofta i någon form av beroendeställning till kommunen/ nämnden/ styrelsen. Att då åberopa samtycke som laglig grund i en sådan situation där det råder ett ojämlikt förhållande mellan parterna, det är inte tillämpbart. Ett samtycke ska dessutom vara frivilligt och kunna återtas och det är sällan frivilligt att som enskild lämna diverse personuppgifter till en kommun/ myndighet.

Den lagliga grund som oftast är aktuell utifrån GDPR för offentlig verksamhet är allmänt intresse och myndighetsutövning. I de fallen måste det som en följd också finnas ett uttryckligt stöd i svensk lagstiftning för hanteringen. Stödet i svensk lagstiftning finns många gånger i verksamhetens specifika lagstiftning som

t ex socialtjänstlagen, skollagen, plan- och bygglagen, kommunallagen, i ett kommunalt reglemente, kollektivavtal osv. Det handlar alltså om att ha en god kännedom om vilket regelverk som styr den egna verksamheten i vilken behandlingen av personuppgifterna förekommer. Dataskyddsombudet noterar att verksamheterna ofta brister i kunskap kring det egna regelverket och att man inte anger det nationella lagstödet i registret.

5.3.2 Avslutande kommentar

Att förstå och tillämpa de olika leden i artikel 30.1 GDPR om behandlingsregister, är inte så enkelt som det kan uppfattas vid en första anblick och det är något som blivit tydligt i samband med genomförd granskning. Dataskyddsombudet bedömer att det finns ett omfattande arbete att göra för att leva upp till kraven i artikel 30 i GDPR. Kunskapen om regelverket och hur praktiskt arbeta med behandlingsregistret är högre idag än 2018-2019 då behandlingarna förtecknades. Så förutsättningarna för arbetet utifrån den aspekten bör vara bättre men då måste verksamheterna avsätta resurser i form av tid och personer som kan arbeta med behandlingsregistren så att de lever upp till GDPRs krav. Ett komplett behandlingsregister utgör även ett värdefullt stöd i det fortsatta arbetet med dataskydd. Ett behandlingsregister som uppfyller kraven är också en förutsättning för att kunna uppfylla informationsplikten och behandla personuppgifter på ett öppet sätt gentemot de registrerade, att hantera de registrerades rättigheter såsom rätten till tillgång (registerutdrag), rätten till rättelse och rätten att göra invändningar.

Grunden till ett bra dataskyddsarbete är att **ha kännedom om verksamhetens personuppgifts-behandlingar**, för att därefter kunna omvandla dessa till tydliga, konkreta och specifika ändamål. Detta kräver god kännedom om den egna organisationen och om de lagar och regler som styr verksamhetens arbete. Det krävs resurser, kunskap och deltagande från de personer som direkt arbetar i kärnverksamheten inom respektive verksamhetsområde i den egna organisationen. Utöver den kunskap som kärnverk-samheten har, krävs även kunskaper i GDPR. Därtill krävs ett arbete för att gå igenom befintliga avtal för att kunna bedöma om det förekommer någon tredjelandsöverföring, genomgång av gallringsbeslut för att kunna precisera lagringstiderna på ett sätt som uppfyller kraven, förtydliga vilka de registrerade är och vilka personuppgifter som behandlas om respektive kategori registrerade samt att identifiera faktiska mottagare, både internt och externt.

För att kunna omhänderta dataskyddsombudets rekommendationer bör arbetet med behandlingsregistret ha hög prioritet inom samtliga nämnder/styrelser med förvaltningar under resterande delen av år 2025.

Jessica Karlsson, dataskyddsombud för kommunerna Falkenberg, Laholm och Hylte