Sveriges Kommuner och Landsting

En vägledning från SKL

Dataskyddsombud i kommuner, landsting och regioner

Dataskyddsförordningen[1] ersätter personuppgiftslagen (PUL) den 25 maj 2018. De nya reglerna börjar då gälla direkt utan någon övergångsperiod.

Reglerna om dataskyddsombud (på engelska Data Protection Officer, DPO) finns i artiklarna 37-39 i dataskyddsförordningen och varje bestämmelse kommenteras separat i vägledningen nedan.

Rollen som dataskyddsombud är inte samma som personuppgiftombudet i nuvarande PUL. Det finns flera skillnader och SKL rekommenderar alla kommuner, landsting och regioner att göra en strategisk bedömning av hur arbetet med dataskyddsfrågor ska genomföras i organisationen. Det är lämpligt att gå igenom avtal och riktlinjer som gäller idag för personuppgiftsombud. Man bör ställa sig frågan om det finns behov av rekrytering för uppdraget som dataskyddsombud och om beskrivningen av uppdraget är i överensstämmelse med de nya kraven i förordningen.

En av de största förändringarna med de nya reglerna är att ombudets kontrollerande och rådgivande funktion för organisationen renodlas. Det innebär samtidigt att organisationen självständigt måste bedriva ett aktivt dataskyddsarbete som inte leds av dataskyddsombudet. Organisationens arbete ska följas upp av ombudet, men det är en rekommendation att varje organisation parallellt med dataskyddsombudet även utser någon i ledningsposition som har ett övergripande ansvar för genomförandet av dataskyddsarbetet.

Ytterligare en förändring är att de nya reglerna ställer krav på dataskyddsombudets kompetens och placering i organisationen. Den person som utses måste ha tillräcklig kunskap om dataskydd och ska utses på grundval av yrkesmässiga kvalifikationer, sakkunskap och förmåga att utföra uppgifterna. Ombudet ska kunna agera självständigt och oberoende i organisationen och ska rapportera till organisationens ledning. Det är därför även en rekommendation att fatta nytt beslut om att utse

[1] http://www.datainspektionen.se/dataskyddsreformen/

dataskyddsombud, även om man bedömer att nuvarande personuppgiftsombud kan fortsätta som dataskyddsombud.

EU-Kommissionen har en Article 29 Data Protection Working Party (WP29) som ger ut råd och vägledningar om hur bestämmelserna ska tillämpas och deras tolkningar kommer att vara vägledande för hur den svenska tillsynsmyndigheten Datainspektionen bedömer dessa frågor. SKLs kommentarer till bestämmelserna stödjer sig på vägledningen om dataskyddsombud; Guidelines on Data Protection Officers (”DPOs”), WP243 rev.01, Adopted on 5 April 2017, http://ec.europa.eu/newsroom/document.cfm?doc_id=44100 , nedan ”Guidelines”.

Hela Dataskyddsförordningen hittas här: http://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Artiklar i Dataskyddsförordningen med kommentarer:

Artikel 37, punkt 1	**Utnämning av dataskyddsombudet** **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,** **b) den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling som, på grund av sin karaktär, sin omfattning och/eller sina ändamål, kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning, eller** **c) den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av uppgifter i enlighet med artikel 9 och personuppgifter som rör fällande domar i brottmål och överträdelser, som avses i artikel 10.**
Kommentar	*Kommuner, landsting och regioner och deras självständiga nämnder är myndigheter och måste utse dataskyddsombud. Det är varje självständig nämnd som är personuppgiftsansvarig för behandlingar inom sitt verksamhetsområde och som ansvarar för*

	att utse ett ombud. Bestämmelsen omfattar även kommunalförbund och gemensamma nämnder. *Även andra aktörer såsom privat, kommunala eller landstingsägda bolag vars verksamhet medför särskilt riskfylld behandlingar ska utse ett dataskyddsombud. Enligt förordning (art. 37.1) är exempel på riskfylld behandling, regelbunden och systematisk övervakning av registrerade i stor skala eller omfattande behandling av känsliga personuppgifter.* *Kommunala eller landstingsägda bolag omfattas inte av uttrycket ”myndighet eller offentligt organ” i GDPR (t.ex. artikel 37, artikel 83 p 7).) I artikel 29- gruppens vägledning om dataskyddsombud sägs, att tolkningen av vad som utgör myndighet eller offentligt organ får göras utifrån nationell lagstiftning.* *Av Datainspektionen hemsida framgår att offentliga organ i Sverige är myndigheter och folkvalda organ: riksdagen, kommunfullmäktige, landstingsfullmäktige och regionfullmäktige samt att privata företag, föreningar och organisationer är inte offentliga organ, och inte heller kommunala eller landstingsägda bolag.* *När det gäller upphandlade privata utförare av kommunal verksamhet bör dessa däremot inte omfattas av definitionen av myndighet eller offentligt organ. Dessa uppdragstagares verksamhet ligger för långt ifrån offentliga funktioner och de kan syssla med mycket som inte är offentligt finansierad verksamhet.* *Privata utförare kan däremot omfattas av någon annan bestämmelse som medför att dataskyddsombud måste utses. Varje personuppgiftsansvarig bör göra sin egen bedömning av detta.* *Reglerna om när dataskyddsombud måste utses innebär en miniminivå och det finns inget som hindrar att andra personuppgiftsansvariga eller personuppgiftsbiträden frivilligt utser dataskyddsombud.*
Artikel 37, punkt 2-4	2. En koncern får utnämna ett enda dataskyddsombud om det på varje etableringsort är lätt att nå ett dataskyddsombud. 3. Om den personuppgiftsansvarige eller personuppgiftsbiträdet är en myndighet eller ett offentligt organ, får ett enda

	dataskyddsombud utnämnas för flera sådana myndigheter eller organ, med hänsyn till deras organisationsstruktur och storlek. 4. I andra fall än de som avses i punkt 1 får eller, om så krävs enligt unionsrätten eller medlemsstaternas nationella rätt, ska den personuppgiftsansvarige eller personuppgiftsbiträdet eller sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden utnämna ett dataskyddsombud. Dataskyddsombudet får agera för sådana sammanslutningar och andra organ som företräder personuppgiftsansvariga eller personuppgiftsbiträden.
Kommentar	*I en kommun, ett landsting eller en region kan ett gemensamt ombud utses för samtliga nämnder inom den kommunen/landstinget om det är lämpligt.* *Flera nämnder i en liten kommun kan t ex utse ett gemensamt ombud, om det är lämpligt utifrån uppgiftens omfattning och komplexiteten i verksamheterna. Om ombudet kan antas kunna fullgöra sina uppgifter för alla myndigheterna och vara lika tillgänglig för de olika personuppgiftsansvariga nämnderna och för registrerade individer. Olika verksamheter kräver olika kunnande hos ombudet.* *Flera kommuner, landsting eller regioner kan även regionalt gemensamt utse ett eller flera ombud som kan arbeta för flera organisationer samtidigt. Detta kan t.ex. vara lämpligt att samordna med kommunförbund eller andra regionala samverkansområden som redan finns.* *Än så länge finns inga begränsningar kopplat till omfattning, antal anställda eller liknande när det gäller hur stor organisation ett dataskyddsombud kan ha. De krav som beskrivs är inriktade på att ombudet ska vara lätt att nå, både inom och utanför organisationen och ombudets möjligheter att genomföra uppdraget. Om ett dataskyddsombud har uppdrag för flera myndigheter med olika typer av verksamheter kan ett team med olika kompetenser ge stöd. Det är den personuppgiftsansvariga organisationens ansvar att se till att ombudet har tillräckliga resurser och tid att klara av uppgifterna.(Guidelines s.10, 22)*
Artikel 37, punkt 5	5. Dataskyddsombudet ska utses på grundval av yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och

	praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som avses i artikel 39.
Kommentar	*Det finns inget formellt krav på att ombudet måste ha viss utbildning eller legitimation, men med tanke på de bedömningar som ska göras enligt artikel 39, kan det vara lämpligt med någon som är jurist eller som har annan relevant utbildning och kunskap och yrkeserfarenhet inom området dataskyddslagstiftning. Förutom juristutbildning kan personer med IT-utbildning, statsvetare, arkivarier eller personer med utbildning inom informationssäkerhet ha goda kunskaper inom detta område.* *Ombudet bör även ha kunskap och förståelse för personuppgiftsbehandling inom sektorn och om IT-system och informationssäkerhet. Eftersom uppdraget är för en myndighet bör ombudet även ha goda kunskaper om förvaltningsregler och verksamhetens processer och rutiner.* *När det gäller förmågan att genomföra arbetsuppgifterna ska det tolkas så att det både ställs krav på personlig lämplighet som hög yrkesmässig integritet och självständighet men även förmågan att klara av uppgifterna beroende på ifall ombudet har fått en lämplig plats i organisationen med tillräckliga resurser.* *Vilken utbildningsnivå och erfarenhet som krävs för att genomföra uppdraget ska även ställas i proportion till hur pass omfattande och hur känslig behandlingen av personuppgifter är, som organisationen genomför.* *Se Guidelines s. 11-12 samt s. 23.*
Artikel 37, punkt 6	6. Dataskyddsombudet får ingå i den personuppgiftsansvariges eller personuppgiftsbiträdets personal, eller utföra uppgifterna på grundval av ett tjänsteavtal.
Kommentar	*Det är tillåtet att anlita utomstående uppdragstagare.* *Om en organisation anlitas som uppdragstagare ska det framgå vilken medarbetare inom den organisationen som har rollen som dataskyddsombud. Uppgifterna får fördelas på ett team av flera medarbetare hos uppdragstagaren så att kunskaper kan*

	kombineras, så länge det är klart vem som har huvudansvar. Detta bör även framgå i avtalet med uppdragstagaren. *Alla medarbetare i teamet måste ha tillräckliga kvalifikationer för uppdraget som dataskyddsombud och man måste även tydliggöra att det inte finns några intressekonflikter på grund av andra uppdrag. Medarbetarna ska även vara skyddade mot att drabbas av negativa påföljder som en följd av sitt arbete som dataskyddsombud. Det är lämpligt att även detta tydliggörs i uppdragsavtalet.*
Artikel 37, punkt 7	7. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till tillsynsmyndigheten.
Kommentar	*Kontaktuppgifter till ombudet måste kommuniceras tydligt så att både tillsynsmyndigheten och enskilda, inom och utanför organisationen, kan nå ombudet.* *Än så länge finns ingen rutin beslutad för anmälan till Datainspektionen.* *Kontaktuppgifterna kan publiceras på organisationens webbplats med telefonnummer, e-postadress, funktionsbrevlåda eller postadress. Det är lämpligt att informera växelfunktioner, registratorer, kontaktcenter eller andra vanliga kontaktvägar.*
Artikel 38	**Dataskyddsombudets ställning**
Kommentar	*Den här bestämmelsen med en tydlig beskrivning av ombudets position i organisationen och utpekat ansvar för personuppgiftsansvarig är ny och innebär en tydlig skärpning jämfört med PuL. De nya reglerna ställer krav på att alla organisationer måste se över sina rutiner när det gäller ombudets placering i organisationen, möjlighet till inflytande, resurser och oberoende ställning.* *Indirekt ställer det även krav på organisationen att ha resurser att vara drivande i dataskyddsfrågor eftersom ombudets roll blir mer tydligt rådgivande och kontrollerande. Det är lämpligt att se över organisationens verksamhetsprocesser som involverar IT och dataanvändning samt vilka ledningsmöten och beslutsgrupper som dataskyddsombudet bör kallas till. Det kan inte förutsättas att*

	ombudet själv ska efterfråga detta efter rekryteringen, utan det ligger på den personuppgiftsansvariga organisationen att förbereda.
Artikel 38, punkt 1	1. Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.
Kommentar	*Det är den personuppgiftsansvariga organisationens ansvar att säkerställa att ombudet involveras och rådfrågas på ett så tidigt stadium som möjligt när personuppgifter ska behandlas.* *Det är avgörande att ombudet involveras i tidigast möjliga skede av alla frågor där dataskydd blir aktuellt. Förutom att rådfrågas i samband med konsekvensbedömningar (se Art 39) ska organisationen säkerställa att dataskyddsombudet till exempel:* - *Regelbundet bjuds in till ledningsmöten på högsta beslutande och mellannivå,* - *Att ombudet närvarar vid beslut som påverkar dataskydd och att all relevant information görs tillgänglig i god tid,* - *Att ombudets bedömning alltid måste övervägas och om ombudets råd inte följs ska organisationen dokumentera skälen.* - *Att dataskyddsombudet omgående kontaktas vid incidenter som kan medföra olovlig åtkomst av information.* *Det är lämpligt att uppdatera interna styrdokument om IT-processer så att det framgår när och hur dataskyddsombudet ska konsulteras.*
Artikel 38, punkt 2	2. Den personuppgiftsansvarige och personuppgiftsbiträdet ska stödja dataskyddsombudet i utförandet av de uppgifter som avses i artikel 39 genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden, samt i upprätthållandet av dennes sakkunskap.
Kommentar	*Organisationen ska från högsta beslutande nivå aktivt tydliggöra sitt stöd för dataskyddsombudet. För kommunledningsnivån bör det*

	vara t.ex. kommundirektör med ledningsgrupp och inom nämnderna förvaltningschef med ledningsgrupp. *De resurser som organisationen ska tillhandahålla för att ombudet ska kunna genomföra uppdraget ska bestå av:* - *Tid; ombudet bör få möjlighet att avsätta tillräckligt med tid för sitt uppdrag. Detta är särskilt viktigt att bevaka när uppdraget är på deltid.* - *Budget* - *Tillgång till stöd från andra kompetenser som HR, juridik, IT, säkerhet och liknande som behövs för att ombudet ska få tillräcklig information,* - *Utbildning; ombudet måste få möjlighet att upprätthålla sin sakkunskap, samt* - *Team; beroende på storlek och typ av organisation bör dataskyddsombudet ha möjlighet att bygga upp ett team för att kunna genomföra uppgifterna.* *Guidelines s. 14 och 23.*
Artikel 38, punkt 3	3. Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att uppgiftskyddsombudet inte tar emot instruktioner som gäller utförandet av dessa uppgifter. Han eller hon får inte avsättas eller bli föremål för sanktioner av den personuppgiftsansvarige eller personuppgiftsbiträdet för att ha utfört sina uppgifter. Dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbiträdets högsta förvaltningsnivå.
Kommentar	*Dataskyddsombudet ska ha en oberoende ställning och ska inte ta emot instruktioner eller utsättas för påtryckningar eller sanktioner som syftar till att påverka hur uppdraget genomförs.* *Ombudet ska rapportera direkt till organisationens högsta förvaltningsnivå, för t.ex. kommuner kommundirektör med ledningsgrupp och inom nämnderna chef för förvaltningen med ledningsgrupp. Det är lämpligt att sätta upp lagom intervall och former för rapportering, en gång om året kan vara för sällan, snarare varje kvartal eller samordnat med andra liknande rapporteringsprocesser.*

	Det finns inget i de nya reglerna som hindrar ett tidsbegränsat förordnande av dataskyddsombudet. Det är en strategisk fråga för varje organisation att bedöma. *Om ombudet anställs i den personuppgiftsansvariges organisation så kan anställningen gälla uppgiften dataskyddsombud eller en annan mer allmän tjänstebeskrivning.*
Artikel 38, punkt 4	4. Den registrerade får kontakta dataskyddsombudet med avseende på alla frågor som rör behandlingen av dennes personuppgifter och utövandet av dennes rättigheter enligt denna förordning.
Kommentar	*Arbetet som dataskyddsombud ska vara delvis utåtriktat så att registrerade individer kan komma i kontakt med ombudet och få hjälp och stöd.*
Artikel 38, punkt 5-6	5. Dataskyddsombudet ska, när det gäller dennes genomförande av sina uppgifter, vara bundet av sekretess eller konfidentialitet i enlighet med unionsrätten eller medlemsstaternas nationella rätt. 6. Dataskyddsombudet får fullgöra andra uppgifter och uppdrag. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska se till att sådana uppgifter och uppdrag inte leder till en intressekonflikt.
Kommentar	*Arbetet som dataskyddsombud kan kombineras med andra uppdrag inom organisationen, men det är direkt olämpligt för t.ex. en IT-chef att vara ombud eftersom det skulle innebära att ombudet granskar sig själv. Det är inte lämpligt att dataskyddsombudets roll blandas med andra uppdrag som är av beslutande eller har ledningskaraktär. Rollen som ombud kan hellre kombineras med uppgifter som rådgivare eller som har kontrollerande funktioner.* *Placeringen i organisationen som beskrivs under Artikel 38 punkt 3 kräver också att ombudet kan ha en självständig och oberoende ställning där denne inte utsätts för påverkan i sitt uppdrag.* *Sammantaget medför detta att det är viktigt att även hitta en lämplig placering i organisationen.*
Artikel 39, punkt 1 a-b	**Dataskyddsombudets uppgifter** 1. Dataskyddsombudet ska ha minst följande uppgifter:

	a) Att informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar om deras skyldigheter enligt denna förordning och andra av unionens eller medlemsstaternas dataskyddsbestämmelser. b) Att övervaka efterlevnaden av denna förordning, av andra av unionens eller medlemsstaternas dataskyddsbestämmelser och av den personuppgiftsansvariges eller personuppgiftsbiträdets strategi för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.
Kommentar	*Dataskyddsombudet ska fungera som intern rådgivare, som ger stöd för den personuppgiftsansvariga kommunen, landstinget eller regionen, så att man förstår hur regelverket ska följas. Detta kräver att ombudet har förmåga att tolka och beskriva detta för organisationens ledning och anställda.* *Ombudet ska även ha en övervakande roll och följa upp att regelverket följs av den personuppgiftsansvariga organisationen.* *Det är dock inte ombudet som ska fungera som projektledare eller som har ansvaret för att ta initiativ, utan rollen liknar mer en revisor eller en controller som löpande granskar verksamheten och kommer med förslag om åtgärder samt rapporterar brister.*
Artikel 39, punkt 1 c	c) Att på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den enligt artikel 35.
Kommentar	*Dataskyddsförordningen Artikel 35 kräver att personuppgiftsansvariga som ska genomföra särskilt känsliga behandlingar av personuppgifter först ska göra en konsekvensbedömning. I det arbetet måste dataskyddsombudet rådfrågas och denne ska även övervaka att åtgärderna genomförs.* *En konsekvensbedömning krävs t ex när det gäller behandling av personuppgifter som avslöjar:* • *ras eller etniskt ursprung,* • *politiska åsikter, religiös eller filosofisk övertygelse eller* • *medlemskap i fackförening och*

	• *behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person,* • *uppgifter om hälsa eller* • *uppgifter om en fysisk persons sexualliv eller sexuella läggning.* *I Artikel 35, punkt 7 beskrivs närmare hur en konsekvensbedömning ska vara utformad. I korthet är det en beskrivning av vilka personuppgifter som ska behandlas, för vilka syften, på vilket sätt, vilka risker det kan medföra och vilka åtgärder som ska vidtas för att minska riskerna.*
Artikel 39, punkt 1 d-e	d) Att samarbeta med tillsynsmyndigheten. e) Att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling, inbegripet det förhandssamråd som avses i artikel 36, och vid behov samråda i alla andra frågor.
Kommentar	*Datainspektionen är tillsynsmyndighet och uppdaterar löpande information för dataskyddsombud och om dataskyddsförordningen.* *http://www.datainspektionen.se/dataskyddsreformen/*
Artikel 39, punkt 2	2. Dataskyddsombudet ska vid utförandet av sina uppgifter ta vederbörlig hänsyn till de risker som är förknippade med behandling, med beaktande av behandlingens art, omfattning, sammanhang och syften.
Kommentar	*Dataskyddsombudet ska vid genomförandet av sitt uppdrag ha ett riskbaserat perspektiv och fokusera på de personuppgiftsbehandlingar som innebär en hög risk för de registrerades personliga integritet.*
Artikel 83, punkt 4 a	4. Vid överträdelser av följande bestämmelser ska det i enlighet med punkt 2 påföras administrativa sanktionsavgifter på upp till 10 000 000 EUR eller, om det gäller ett företag, på upp till 2 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst: a) Personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter enligt artiklarna 8, 11, 25–39, 42 och 43.
Kommentar	*Personuppgiftsansvariga organisationer som är skyldiga att utse dataskyddsombud, men inte gör det, kan drabbas av sanktionsavgifter.*

	För svenska myndigheter, inklusive kommuner, landsting och regioner, gäller dock inte reglerna om sanktionsavgifter direkt enligt förordningen. Medlemsländerna får var och en enligt artikel 83.7 i förordningen ta ställning till om sanktionsavgifter skall gälla för offentliga myndigheter och organ eller inte och i så fall vilka belopp som ska gälla. I Sverige är detta ännu inte beslutat. Förslagen i den nya s.k. dataskyddslagen (SOU 2017:39) skulle om de beslutas, innebära sanktionsavgifter för myndigheter med max belopp om 10 miljoner kr när det gäller bestämmelser om dataskyddsombud.