Avdelningen för Digitalisering

Instruktion till mall för registerförteckning

Dataskyddsförordningen artikel 30.1 kräver att varje personuppgiftsansvarig organisation ska föra ett register över personuppgiftsbehandlingar som utförs i den verksamhet som den personuppgiftsansvarige ansvarar för. När dataskyddsförordningen börjar gälla den 26 maj 2018 ska denna förteckning finnas på plats.

SKL har tagit fram en mall som kan användas för att föra denna förteckning, se Excel-dokument ”**SKL-MALL FÖR REGISTERFÖRTECKNING**”. Det finns även verktyg för detta ändamål som kan upphandlas.

Detta krävs av varje personuppgiftsansvarig organisation:

- Upprätta en förteckning över personuppgiftsbehandlingar i verksamheten.
- Skapa rutiner för att kunna hålla förteckningen uppdaterad.
- Förteckningen ska hållas skriftligt och i elektronisk form.
- Förteckningen ska vid begäran kunna visas upp för tillsynsmyndigheten (Datainspektionen).

Nedan följer förklaring och kommentarer avseende de begrepp och kategorier som finns med i mallen.

De kategorier som har markerats med * är obligatoriska att fylla i enligt artikel 30.1. Övriga kolumner är bra att ha, men kan tas bort eller anpassas till vad som fungerar lokalt.

Definitioner av vissa grundläggande begrepp finns i dataskyddsförordningens artikel 4. Hela förordningstexten kan läsas i webbversion här: http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/

Begrepp /kategori i MALLEN	Kolumn	Ordförklaring och kommentar
Löpnummer/ Beteckning/ ID	A	Här finns plats att ange samma beteckning som används i andra förteckningar, t.ex. listor över verksamhetssystem eller liknande.
Personuppgiftsansvarig*	B	För kommuner, landsting och regioner är det varje nämnd som har självständigt verksamhetsansvar som räknas som personuppgiftsansvarig.

Sveriges Kommuner och Landsting
Post: 118 82 Stockholm, *Besök:* Hornsgatan 20
Tfn: växel 08-452 70 00, *Fax:* 08-452 70 50
Org nr: 222000-0315, info@skl.se, www.skl.se

		För behandlingar som är gemensamma för hela organisationen, som t.ex. e-post eller personaladministrativa system, bör kommunstyrelse eller annan övergripande nämnd vara ansvarig. Varje organisation kan själv välja om förteckningen ska föras gemensamt eller om den ska finnas hos varje nämnd. Det som måste anges är: - Namn på personuppgiftsansvarige, t.ex. Fastighetsnämnden i Mittköpings kommun. - Kontaktuppgifter, postadress, mail-adress till nämndens förvaltning. - Den personuppgiftsansvariges företrädare, t.ex. ansvarig i ledningen eller utsedd kontaktperson utöver dataskyddsombudet. - Dataskyddsombudet, med kontaktuppgifter. - Ifall det finns gemensamt personuppgiftsansvariga, om man genomför behandlingar gemensamt med annan organisation, kontaktuppgifter även till dem.
Behandlingens namn	C	Som *behandling* räknas en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring. Det kan vara svårt att särskilja en behandling från en annan och se var gränserna går. Ett råd är att så långt möjligt följa den struktur

		som finns i verksamhetssystemen och att samla behandling av personuppgifter som kan sammanföras under samma ändamål och där det rör samma kategorier av personuppgifter, till en behandling. Om det finns flera behandlingar inom ramen för samma verksamhetssystem bör man döpa dem till olika namn, t.ex. ”Skolsystemet planeringsverktyget” respektive ”Skolsystemet elevdokumentation”. Undersök gärna ifall behandlingar med olika behov av säkerhetsåtgärder kan segmenteras eller hanteras med olika nivå av säkerhet inom ramen för samma verksamhetssystem. Om det inte är möjligt, måste de känsligaste personuppgifternas behov av säkerhet och skyddsåtgärder bli styrande för helheten.
Personuppgift ***(denna finns inte med som en kolumn i mallen för registerförteckning, utan anges som ordförklaring)***	--	Som *personuppgift* räknas varje upplysning som avser en identifierad eller identifierbar fysisk person, som direkt eller indirekt kan identifieras med hjälp av namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.
Ingår i system	D	Det är praktiskt att ange i vilket verksamhetssystem som personuppgiftsbehandlingen sker. Det ger även möjlighet till enkel sortering i förteckningen.
Beskrivning av ändamålen med behandlingen*	E	Ändamålen med behandlingen ska enligt artikel 5.1 b) vara ”särskilda, uttryckligt angivna och berättigade”. För ett personalsystem kan man t.ex. ange: ”Behandling av uppgifter om medarbetare för löneadministration, planering och

		uppföljning samt hantering av personalärenden.” Var hellre mer detaljerad i beskrivningen än att skriva för kortfattat. Beskrivningen av ändamålen med behandlingen ska också fungera som underlag för att kunna säkerställa att behandlingen är tillåten enligt någon av de tillåtna ändamål som ges i dataskyddsförordningen. Beskrivningen av ändamålen är även viktig eftersom personuppgifterna normalt inte får behandlas för något annat ändamål i ett senare skede. Om ändamålet beskrivs för snävt från början kommer det att ”låsa” personuppgifterna framåt i tiden. Diskutera gärna beskrivningen av ändamålen så att beskrivningen omfattar verksamhetens behov men ändå uppfyller kravet på att ändamålen ska vara ”särskilda”.
Behandlingen omfattar kategorier av registrerade personer*	F	Här ska man dokumentera vilka personer det är som blir registrerade, t.ex. medarbetare, elever, sökande inom försörjningsstöd, låntagare på biblioteket, osv.
Behandlingen omfattar följande typer av personuppgifter*	G	Här ska man dokumentera vilka olika typer av personuppgifter som registreras om individerna, t.ex. för sökande inom försörjningsstöd: Namn, personnummer, adress, inkomstuppgifter, uppgift om anhöriga, underlag för bedömning som kan omfatta hälsouppgifter, intyg som kan omfatta hälsouppgifter, beslut. Försök att vara så detaljerad som möjligt eftersom det måste framgå om det kommer att finnas känsliga personuppgifter (särskilda kategorier av uppgifter).
Förekommer särskilt känsliga	H	Om det förekommer ”särskilda kategorier av personuppgifter” även kallade känsliga

personuppgifter och vilka?		personuppgifter, ange vilka typer av sådana uppgifter det rör sig om. Detta är inte en obligatorisk uppgift, men det kan vara praktiskt att dokumentera och det blir lättare kunna sortera fram i förteckningen vilka behandlingar som omfattar känsliga uppgifter. Se nedan vilka typer av uppgifter det gäller.
Särskilda kategorier av personuppgifter (denna finns inte med som en kolumn i mallen för registerförteckning, utan anges som ordförklaring)	--	För särskilda kategorier av (känsliga) personuppgifter finns krav på extra bedömning av om och för vilka syften sådana uppgifter får behandlas (artikel 9) och krav på att göra en konsekvensbedömning avseende dataskydd (artikel 35). ***Som särskilda kategorier av personuppgifter räknas:*** - uppgifter som avslöjar ras eller etniskt ursprung, - politiska åsikter, - religiös eller filosofisk övertygelse eller - medlemskap i fackförening och - behandling av genetiska uppgifter eller - biometriska uppgifter för att entydigt identifiera en fysisk person, - uppgifter om hälsa eller - uppgifter om en fysisk persons sexualliv eller sexuella läggning Det finns även liknande restriktioner för behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder (artikel 10).
Kategorier av mottagare av personuppgifterna internt och externt*	I	Här ska man dokumentera vilka olika typer av mottagare som uppgifterna lämnas ut till, t.ex. Skatteverket, Polismyndigheten, Kriminalvården, Landstinget (enhet), Skolverket, osv. Från definitionen av ”mottagare” i artikel 4:

		”en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas..” Det är obligatoriskt att ange externa mottagare och det är en rekommendation att även ange mottagare internt i den egna organisationen. Detta för att lättare kunna uppfylla krav på att i efterhand spåra uppgiftsflöden, genomföra rättelser och inte minst viktigt – kunna säkerställa att personuppgifterna inte riskerar att användas för nya ändamål som inte stämmer överens med de som gällde då uppgifterna samlades in.
Dokumentation om överföring av personuppgifter sker till tredje land*	J	Om personuppgifter kommer att överföras till tredje land ska en särskild dokumentation finnas om detta. Som tredje land räknas länder utanför EU och EES-samarbetet. Om sådan överföring är aktuell, krävs särskild bedömning, läs mer i artiklarna 44, 45, 46 samt på Datainspektionens webbplats, tills vidare information som avser nuvarande lagstiftning, PuL: http://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/#tredjeland
Tidsfrister för radering*	K	För dokumentation i denna kolumn krävs en analys av hur länge personuppgifterna i varje behandling ska behandlas i identifierbar form. I artikel 5.1 e) införs en ny princip ”lagringsminimering”. Den innebär att personuppgifter inte får lagras i identifierbar form längre än vad som är nödvändigt i förhållande till ändamålen. De tidsfrister som beslutas ska även dokumenteras i förteckningen och i gallringsbeslut för myndigheten, så att radering eller avidentifiering kan genomföras när personuppgifterna inte längre behövs. Av

		artikel 89.1 framgår att personuppgifter kan tas bort genom pseudonymisering. Personuppgifter får dock lagras under längre perioder om personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1.
Ange vilka lagliga grunder som finns för behandlingen	L	Detta är ingen obligatorisk punkt att ha med i registerförteckningen, men det är nödvändigt att någonstans dokumentera och kunna redovisa vilka lagliga grunder som finns så vi föreslår att detta görs här. Notera att det kan vara nödvändigt att ange laglig grund först för ”grundnivå”, dvs. behandling som är tillåten enligt artikel 6. Om det även förekommer känsliga – särskilda kategorier av – personuppgifter eller uppgifter om fällande domar i brottmål m.m. ska behandlingen av dem dessutom vara tillåten enligt någon av artiklarna 9-10.
Allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder*	M	Här anges i artikel 30.1 g) att man ”om möjligt” ska lämna en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1. Detta är alltså inte en absolut plikt att redovisa varje detalj i säkerhetsåtgärderna i förteckningen, utan det bör räcka att göra en översiktlig beskrivning och kanske hänvisa till att säkerhetsåtgärderna finns dokumenterade på annat ställe.
Om personuppgiftsbiträden anlitas för att genomföra behandlingen, ange namn och kontaktuppgifter till dessa leverantörer	N	Det kan vara praktiskt att ange kontaktuppgifter till personuppgiftsbiträdet eller en referens till avtal, eller liknande, men det är inte obligatoriskt att ha med i förteckningen.