SUNDSVALLS KOMMUN

Handbok för arbete med kvalificerad, säker och långsiktig Informationsförvaltning

Titel:	**Informationsförvaltningshandbok**		
Version:	2.0		
Skriven av:	Petronella Enström, IT-strateg, Koncernstaben	Datum:	2017-07-22
Godkänd av:	TF IT-direktör, Linda Gustafsson	Datum:	2017-08-17

Innehållsförteckning

Förändringshistorik

Version	Datum	Förändringsorsak	Utfärdare
1.0	2012-12-18	Behandlad i IT-rådet, beslutat chef IT-stab	Petronella Enström
2.0	2017-08-17	Behandlad i styrgrupp för HIT fas 1, beslutad av TF IT-direktör	Petronella Enström

Relaterade dokument

Version	Datum	Benämning	Beslutsinstans
1.0	2011-02-28	IT-strategi	Kommunfullmäktige
1.3	2011-09-15	Systemförvaltningshandbok	IT-stab
1.0	2008-12-30	Mall för systemförvaltningsplan	Chef IT-stab
1.0	2009-05-25	Modell för klassificering av information, rekommendationer, MSB 0040-09	MSB och SIS
	2011-12-15	Verksamhetsanalys, ramverk för informationssäkerhet	MSB
	2016	SKL:s verktyg KLASSA	SKL
1.0		Riktlinje för informationsmodeller i Sparx EA	
1.1		Riktlinjer vid val av molntjänst	
o.2		Riktlinjer informationssäkerhetsklassning	
		Bruttolista krav vid upphandling, Teknik och informationssäkerhet	
		Riktlinjer för hantering av inbrottslarm, passersystem och nycklar	

1 Inledning

Detta dokument är Sundsvalls kommunkoncerns informationsförvaltningshandbok.

I IT-strategin fastställs att en kvalificerad informationsförvaltning krävs. I takt med att allt mer information digitaliseras så ökar också kravet på hög tillgänglighet och hög kvalitet på efterfrågad information.

Information i alla dess former är en viktig tillgång i samhället och behöver lämpligt skydd. Framväxten av ett samhälle som i ökad omfattning bygger på att information hanteras elektroniskt skapar behov av modeller och metoder för att lägga grunden till detta skydd. Om information ska utbytas och förmedlas säkert måste det finnas gemensamma modeller för att värdera information för att så långt det är möjlig skapa skyddsnivåer som överensstämmer.

Det är viktigt att ta tillvara informationens värde. Det görs genom en kvalificerad, säker och långsiktig informationsförvaltning. Syftet med informationsförvaltning är primärt att stödja ett effektivt genomförande av det uppdrag som kommunkoncernen är satt att sköta. Informationsförvaltning innebär att kartlägga, planera, skydda och anpassa informationstillgångarna så att verksamheterna kan arbeta på ett effektivt sätt med sitt uppdrag och mot sina mål. Detta bland annat för ett bättre nyttjande av information och säkerställa informationssäkerheten som grund för e-förvaltning och e-tjänster.

2 Målgrupp

Målgruppen för detta dokument är de roller som ansvarar och arbetar med kvalificerad, säker och långsiktig informationsförvaltning i kommunkoncernen.

3 Informationsförvaltningens omfattning

Med informationsförvaltning avses förvaltning av information som används inom Sundsvalls kommunkoncern.

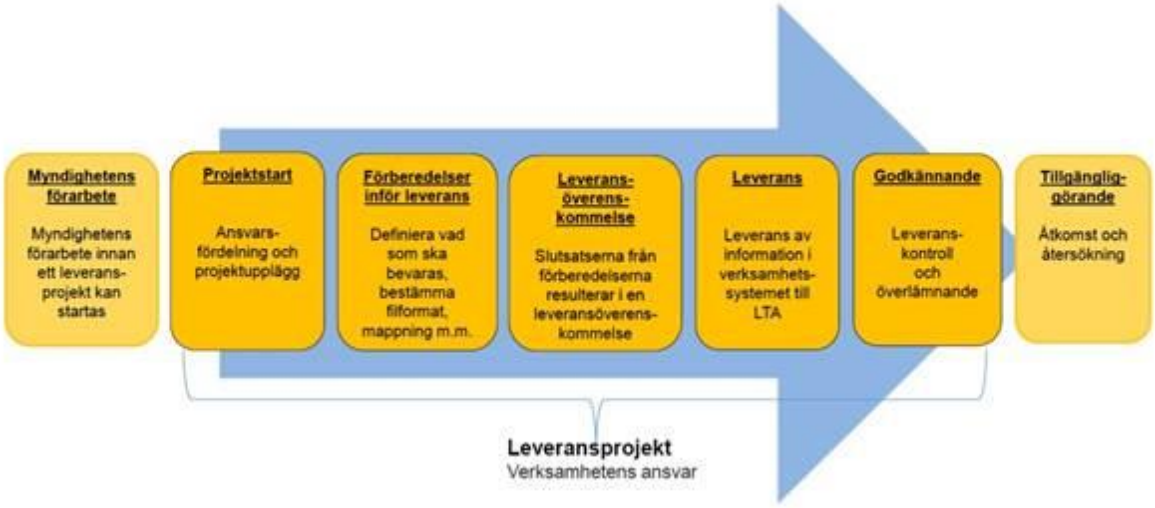
3.1 Personuppgifter

Den informationsmängd som förvaltas inom kommunkoncernen innehåller i de flesta fall personuppgifter. Det juridiska begreppet personuppgift är vitt och avser varje information som direkt eller indirekt kan identifiera en levande person. En personuppgift kan vara till exempel adressuppgifter, telefonnummer, namn, personnummer, fingeravtryck, genetiska uppgifter o.s.v. Begreppet personuppgift omfattar även information som isolerat inte kan identifiera levande personer, men som tillsammans med annan information kan identifiera levande personer. Exempelvis är yrkeskategorin ”ingenjör*”* inte en personuppgift i sig själv, men om yrkeskategorin ”ingenjör” samkörs med information om en organisation med *en* (1 st) anställd ingenjör så finns möjlighet att identifiera en levande person. Därmed är Yrkeskategorin ”ingenjör” att klassa som en personuppgift.

3.2 Bevarande eller gallring

Information arkiveras för att tillgodose förutom verksamheten även allmänhetens och forskningens behov. Det regleras av Offentlighetsprincipen och dess tillhörande lagstiftning. All information kan och behöver inte sparas. För att kunna avgöra vad som ska bevaras respektive gallras krävs kunskap om vilken information som finns och hur den är strukturerad.

Varje verksamhet är skyldig att ha en aktuell dokumenthanteringsplan där det regleras. Den ska vara beslutad i respektive nämnd/styrelse och vara godkänd av arkivmyndigheten. Informationen om vad som gallras ska dokumenteras för att uppfylla spårbarhetskravet. Även vid förberedande av arkivering till e-arkiv gäller ovanstående. Under alla omständigheter måste rätt beskrivande data sättas för att informationens kontext inte ska gå förlorad.



4 Roller och ansvar

Informationsförvaltning omfattar många roller några beskrivs nedan.

4.1 Informationssäkerhetssamordnare

Informationssäkerhetssamordnaren samordnar informationssäkerhetsarbete för hela Kommunkoncernen. Arbetet bedrivs enligt standarden ISO 27000.

- Håller ledningens genomgång av informationssäkerhet
- Framtagande av ett regelverk för informationssäkerhet
- Tillhandahåller metod för informationssäkerhetsklassning
- Tillhandahåller informationssäkerhetskrav vid användning av IT-stöd
- Tillhandahåller informationsmaterial om informationssäkerhet
- Sammankallande till arbetsgrupp för strategisk informationssäkerhet

4.2 IT-säkerhetsansvarig

IT-säkerhetsansvarig ansvarar för IT-säkerhet i kommunkoncernens IT-infrastruktur och levererade tjänster enligt standard ISO 27000.

- Ansvarig för IT-säkerheten i kommunens IT-infrastruktur, IT-drift och levererade tjänster enligt definierad tjänstekatalog
- Tillhandahåller regler för IT-användning till medarbetare
- Tillhandahålla krav rörande IT-säkerhet gentemot IT-leverantörer av IT-stöd för användning i exempelvis upphandling

4.3 Säkerhetsansvarig för fysisk säkerhet

- Ansvarar för ”Riktlinjer för hantering av inbrottslarm, passersystem och nycklar”.
- Behovsbedömning avseende inbrottslarm och brandlarm samt framtagande av förslag på säkerhetsnivå.
- Behovsbedömning av mekaniskt skydd av fastighet samt framtagande av förslag på säkerhetsnivå.
- Framtagande av rätt säkerhetsklass på säkerhetsskåp och dokumentskåp
- Framtagande av förslag till rätt dokumentförstörare, då de har olika säkerhetsklassningar

4.4 Ansvar för informationsarkitektur

Rollen har ett övergripande strategiskt ansvar för informationsinfrastrukturen, gäller hela kommunkoncernen med bolag och räddningstjänst.

- Tillhandahåller metod för informationsförvaltning
- Tillhandahåller metod för informationsmodellering
- Tillhandahåller informationsmaterial om informationsförvaltning
- Tillhandahåller katalog över tillgängliga informationstjänster
- Tillhandahåller modellbibliotek för informationsarkitektur
- Definierar strategiska informationstillgångar
- Definierar gällande datalager

4.5 Informationsägare

Informationsägare är förvaltningschef eller motsvarande om denne ej delegerat uppgiften till annan part inom sin verksamhet. Informationsägaren äger informationen och ska se till att informationen förvaltas säkert, kvalificerat och långsiktigt på bästa sätt för att ge maximal nytta enligt informationsförvaltningsmodellen.

Informationsägaren bör utse en informationsförvaltare som arbetar operativt med informationsförvaltning. Informationsägare är den som äger och ansvarar för att informationen är riktig och tillförlitlig samt för det sätt informationen sprids. Informationsägaren är därmed riskägare för den information som ska hanteras i it-stöd. För att hantera risken bör informationsägaren genomföra en riskanalys. Eftersom skadeverkningarna av bristande säkerhet i it-stöd uppstår hos informationsägaren är det informationsägaren som måste bedöma risker och ställa krav bland annat genom informationssäkerhetsklassning.

Då det gäller IT-stöd finns det en systemägare och dess relation till informationsägare är att det kan finnas flera informationsägare som har information i samma IT-stöd, eller att flera IT-stöd använder samma information. Systemägare och informationsägare kan vara samma person. De interna relationerna mellan informationsägare och systemägare bör, när det gäller informationssäkerhet, utgå från informationsägaren.

- Äger informationen
- Äger informationsmodellen
- Ansvarar för att informationen följer lagar, förordningar och interna styrdokument.
- Ansvarar för informationssäkerhetsklassning.

- Ansvarar för avtal och överenskommelser med informationsleverantör där det förekommer
- Ansvarar för avtal och överenskommelser med systemägare som vill nyttja informationen d.v.s. distribution och integration.
- Ansvarar för arkivering och gallring och att besluten dokumenteras.
- Beslutar om informationsförvaltningsplan

4.6 Informationsförvaltare

Informationsförvaltaren ska arbeta utifrån informationsägarens mål i mycket nära kontakt med verksamheten.

Då det gäller IT-stöd finns det en systemförvaltare och dess relation till informationsförvaltare är att det kan finnas flera informationsförvaltare som har information i samma IT-stöd, eller att flera IT-stöd använder samma information. Vidare kan systemförvaltare och informationsförvaltare vara samma.

- Upprätta informationsförvaltningsplan till informationsägaren enligt dennes mål
- Ansvarar för att informationen följer informationsförvaltningsplanen.
- Rapporterar arbetet med informationsförvaltningsplanen till informationsägaren
- Ansvarig för uppföljning av ev. avtal och överenskommelser med ev. informationsleverantör
- Ansvarig för uppföljning av ev. avtal och överenskommelser med systemförvaltaren för IT-stöd som nyttjar informationen.

4.7 Kommunarkivarie

Kommunarkivarien har rollen som Arkivmyndighetens ombud. Rollen verkar mot verksamheten, allmänheten och forskningens intressen.

- Tillsyn av informationshantering enligt reglerna i offentlighets- och sekretesslagen.
- Verkar för att informationen i kommunens olika verksamheter är åtkomlig för allmänheten.
- Råd och stöd till verksamheten kring vad som kan gallras.
- Råd och stöd till verksamheten kring vad som ska bevaras och varför det ska bevaras leder till beslut hur det ska bevaras.
- Godkänna gallring av information och dokumentering av gallring.

Ett perspektiv är att informations- och informationssäkerhetsklassningen ligger till grund för långsiktigbevarande i e-arkiv för att ge rätt tillgänglighet.

4.8 Personuppgiftsansvarig

Rollen som personuppgiftsansvarig är frånkopplad övriga roller som nämns i handboken. Det är normalt juridiska personer som kan inneha rollen som personuppgiftsansvar, d.v.s. aktiebolag, förening, *eller* myndighet osv. Undantagsvis kan en fysisk person vara personuppgiftsansvarig, exempelvis en enskild företagare.

Enligt personuppgiftslagen och den kommande dataskyddsförordningen definieras den personuppgiftsansvarige som den som bestämmer *ändamålen och medlen* för behandlingen av

personuppgifter. I en kommun är normalt både kommunstyrelsen och de kommunala nämnderna personuppgiftsansvariga för de behandlingar som de har att utföra inom sin egen verksamhet. Men detta kan variera och de faktiska omständigheterna måste prövas i varje enskilt fall, till exempel utifrån om nämnden självständigt förfogar över de personuppgifter som behandlas. Det är dock alltid *styrelsen/*nämnden som helhet som är att se som personuppgiftsansvarig*. och inte en enskild enhet inom styrelsen/nämnden eller en enskild person såsom t.ex. chefen för respektive nämnd. Det viktiga i sammanhanget är alltså att utröna vem som bestämmer*.

Ledande frågor att ställa för att utröna vem som bestämmer *ändamålen och medlen* för behandlingen av personuppgifter:

- vem/vilka som har bestämt hur uppgifterna ska hanteras?
- vem/vilka har rätt att självständigt ändra, komplettera och radera uppgifter?

Om två eller flera nämnder bestämmer ändamålen och medlen för *samma* uppgifter är dessa att betrakta som personuppgiftsansvariga tillsammans, d.v.s. det föreligger ett delat personuppgiftsansvar.

Den personuppgiftsansvarige ansvarar för att följa gällande lagstiftning för personuppgiftshantering och även kommande lagstiftning (dataskyddsförordningen) vilket bl.a. omfattar *(dock inte uttömmande):*

- Ansvar för att tillgodose de registrerades rättigheter (såsom rätten till information, radering, rättelse, rätten att göra invändningar mot behandlingen o.s.v.).
- Ansvarar för att personuppgifter finns dokumenterade i register över personuppgiftsbehandlingar
- Ansvar för att personuppgiftsbehandlingen uppfyller minst en rättslig grund.
- Ansvar för att inte senare behandla personuppgifter för ändamål som skiljer sig från de ändamål för vilka uppgifterna samlades in (finalitetsprincipen).
- Ansvar för att skriva biträdesavtal (vid en biträdesrelation).
- Ansvar för att säkerställa att IT-systemen uppfyller de tekniska krav som följer av den kommande dataskyddsförordningen.
- Ansvar för att utse ett personuppgiftsombud (personuppgiftslagen).
- Ansvar för att utse ett dataskyddsombud (dataskyddsförordningen).
- Ansvar för att dataskyddsombudet ska kunna delta i alla frågor som rör skyddet av personuppgifter, tillhandahålla alla resurser som ombudet behöver för att kunna fullgöra sitt uppdrag, se till att dataskyddsombudet kan inta en oberoende ställning för att kunna fullgöra sitt uppdrag på ett objektivt sätt.

4.9 Personuppgiftsbiträde

Ett personuppgiftsbiträde definieras som en fysisk eller juridisk person, offentlig myndighet eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Om den personuppgiftsansvarige till exempel lagrar sina uppgifter hos en extern molntjänstleverantör är leverantören att betrakta som biträde. Om en extern leverantör på andra sätt nyttjar den personuppgiftsansvariges uppgifter å den personuppgiftsansvarige vägnar är leverantören också att betrakta som biträde, exempelvis om kommunen ber en

extern leverantör analysera viss information som innehåller personuppgifter som kommunen tillhandahåller.

Ett personuppgiftsbiträde ansvarar bland annat för att:

- Behandla personuppgifter enligt instruktion från den personuppgiftsansvarige.
- Inte behandla personuppgifter för egna intressen, d.v.s. inte behandla uppgifterna för ändamål som inte överensstämmer med instruktionen från den personuppgiftsansvarige.
- Inte utse ett eget personuppgiftsbiträde som behandlar den personuppgiftsansvariges personuppgifter utan ett godkännande från den personuppgiftsansvarige.
- Uppfylla de nya tekniska lagkrav som riktar sig direkt mot personuppgiftsbiträdet (dataskyddsförordningen).
- Föra register över personuppgiftsbehandlingar (dataskyddsförordningen).
- Utse ett dataskyddsombud (dataskyddsförordningen).
- Dataskyddsombudet ska kunna delta i alla frågor som rör skyddet av personuppgifter, tillhandahålla alla resurser som ombudet behöver för att kunna fullgöra sitt uppdrag, se till att dataskyddsombudet kan inta en oberoende ställning för att kunna fullgöra sitt uppdrag på ett objektivt sätt.

4.10 Personuppgiftsombud

Enligt nuvarande personuppgiftslag ska personuppgiftsombudet granska den personuppgiftsansvariges verksamhet. Uppdraget kan jämföras med ett revisorsuppdrag. Ett personuppgiftsombud är alltid en fysisk person till skillnad från den personuppgiftsansvarige.

Personuppgiftsombudet ansvarar för att:

- Se till att den personuppgiftsansvarige behandlar personuppgifter på ett lagligt och *ett* korrekt sätt och i enlighet med god sed samt påpeka eventuella brister för den personuppgiftsansvarige.
- Anmäla misstänkta brister eller överträdelser till datainspektionen.
- Samråda med datainspektion vid tveksamheter om hur de bestämmelser som gäller för personuppgiftsbehandling ska tillämpas.
- Hjälpa de registrerade att få rättelse om deras personuppgifter misstänks behandlas felaktigt eller ofullständigt.

4.11 Dataskyddsombud

Enligt dataskyddsförordningen ersätts personuppgiftsombud med ett s.k dataskyddsombud. Det är obligatoriskt för myndigheter att utse ett dataskyddsombud. Ett och samma dataskyddsombud kan arbeta i olika myndigheter samtidigt, d.v.s. det är *enligt bestämmelserna i dataskyddsförordningen* tillräckligt med ett dataskyddsombud för hela kommunkoncernen.

En annan nyhet är att Även myndigheter som är att betrakta som personuppgiftsbiträden *också* ska utse ett dataskyddsombud. Dataskyddsförordningen ställer högre kompetenskrav på dataskyddsombudet till skillnad från det nuvarande personuppgiftsombudet.

Dataskyddsombudet ska besitta yrkesmässiga kvalifikationer och sakkunskaper om lagstiftning och praxis avseende dataskydd. Dataskyddsombudet behöver inte ingå i den personuppgiftsansvariges eller personuppgiftsbiträdes ordinarie personal utan det är möjligt att tilldela uppdraget till en extern resurs.

Dataskyddsombudet ansvarar för att:

- Rapportera brister till högsta förvaltningsnivå.
- Övervaka efterlevnaden av dataskyddsförordningen och annan lagstiftning som rör behandling av personuppgifter.
- Agera kontaktperson för de registrerade för att kunna besvara alla frågor som rör behandling av deras personuppgifter.
- Informera och utbilda personalen rörande dataskyddsfrågor.
- Ge råd vad gäller konsekvensbedömning.
- Samarbeta med tillsynsmyndighet (troligtvis datainspektionen) samt agera kontaktpunkt för tillsynsmyndigheten.

5 Informationssäkerhetsarbete

Då det gäller informationssäkerhet är det av stor vikt att arbete sker både inom enskild verksamheter men även verksamhetsövergripande. Därför finns en arbetsgrupp för strategisk informationssäkerhet där verksamhetsövergripande och strategiska frågor rörande informationssäkerhet behandlas. Arbetsgruppen ska ses som en motor för att driva mot en kvalificerad, säker och långsiktig informationsförvaltning i koncernen.

Arbetsgruppens medlemmar använder sig av sina etablerade nätverk för att koordinera och informera om frågor rörande informationssäkerhet inom sina kompetensområden.

Arbetsgruppen består av följande roller som med sina kompetensområden bidrar till en helhetssyn rörande informationssäkerhet i koncernen:

- Informationssäkerhetssamordnare
- Säkerhetsansvarig för fysisk säkerhet
- Dataskyddsombud
- Kriskommunikatör
- Kommunarkivarie
- IT-säkerhetsansvarig
- Ansvarig för informationsarkitektur
- HR-strateg

Respektive roll deltar utifrån sin roll och kan fatta beslut utifrån sitt enskilda beslutsmandat, arbetsgruppen har inget eget beslutsmandat.

6 Informationsförvaltningsplan

Informationsförvaltningsplaner ska upprättas för:

- information som många verksamheter använder tex fastighetsregister, befolkningsdata

- information som anses vara verksamhetskritiskt eller delas av flera förvaltningar, bolag eller IT-stöd.
- Verksamhetsinformation, framför allt inför upphandling av verksamhetsystem eller leverans till e-arkiv

Digital information som endast hanteras av ett IT-stöd kan hanteras i IT-stödets systemförvaltningsplan med vissa tillägg, t.ex. hantering av personuppgifter, informationssäkerhetsklassning och behörighetsroller.

Informationsförvaltningsplanen beskriver bland annat:

- Informationen, dess nytta och informationsförvaltningens omfattning.
- Informationsmodell, begreppsmodell och definitioner.
- Informationsflöde.
- Informationssäkerhetsklassningens resultat, risk- och hotanalys.
- Hantering av ev. personuppgifter.
- Informationens processtillhörighet (punktnotation).
- Informationens integration i IT-stöd och överenskommelser eller avtal.
- Informationsförvaltningens organisation, roller, samverkan och uppföljning.
- Bevarande eller gallring, arkivering.
- Utveckling, vilka behov finns och vilka planerade aktiviteter kommer att genomföras.

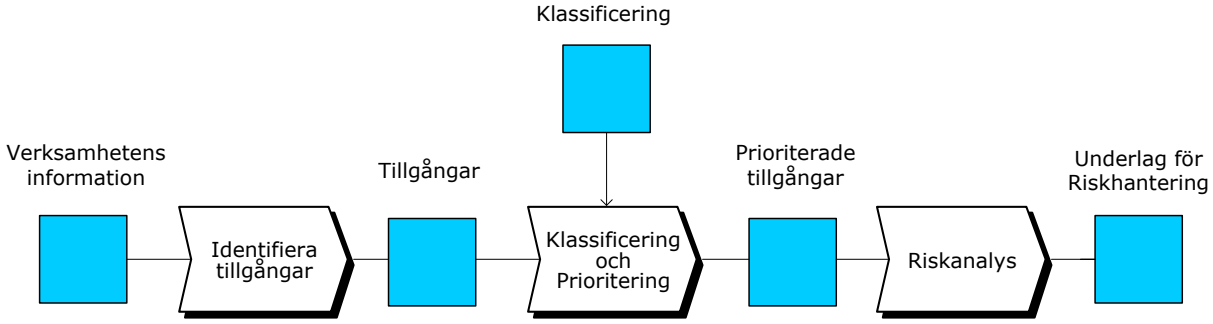
Det finns en modelleringshandbok som stöd för att rita processer på olika nivåer.

6.1 Informationsmodell

En informationsmodell med tillhörande definitioner ska dokumenteras enligt Riktlinje för informationsmodeller i Sparx EA.

Definition informationsmodell: En informationsmodell är resultatet av en informationsmodellering i verksamheten. Den visar verksamhetens information. En informationsmodell beskriver hur informationen är strukturerad.
Definition datamodell: En beskrivning av hur databaserna och dess tabeller är organiserade i ett IT-system.

6.2 Informationssäkerhetsklassning och risk- och sårbarhetsanslys



Informationssäkerhetsklassning ska genomföras i verksamheten och dokumenteras. Informationssäkerhetsklassning görs utifrån aspekterna konfidentialitet, riktighet, tillgänglighet och spårbarhet. Se Riktlinje för informationssäkerhetsklassning.

Efter det gör verksamheten en risk- och sårbarhetsanslys, åtgärder för att eliminera risker planeras och slutligen görs en acceptans av kvarvarande risker av Informationsägare. Rekommendationen är att använda MSB vägledningar.

Detta arbete blir ett bra underlag till en kontinuitetsplanering för verksamheten för att kunna upprätthålla sin verksamhet vid en informationssäkerhetsincident.

6.3 Personuppgiftsbiträdesavtal

Mellan den personuppgiftsanvarige och personuppgiftsbiträdet ska det enligt 30 § 2 st. PuL, motsvarande bestämmelse finns i dataskyddsförordningens artikel 28 p.3, upprättas ett personuppgiftsbiträdesavtal.

Avtalet ska föreskriva att personuppgiftsbiträdet bara får behandla de aktuella personuppgifterna i enlighet med den personuppgiftsansvariges instruktioner och att personuppgiftsbiträdet är skyldig att vidta de säkerhetsåtgärder som stadgas i PuL och motsvarande bestämmelser i dataskyddsförordningen. Till exempel ska ett biträdesavtal skrivas vid användande av molntjänstleverantör.

Biträdesavtalet reglerar specifikt skyddet av personuppgifter och återfinns ofta som bilaga till det övergripande leverantörsavtalet. Det är den personuppgiftsansvarige som ska se till att personbiträdesavtal finns på plats och att avtalsvillkoren stämmer överens med de lagkrav som gäller för ett biträdesavtal.

6.4 Arkivering

Arkivhanteringen styrs av lagar och förordningar. Ärenden och dess handlingar ska gallras eller arkiveras enligt fastställda rutiner. Dessa ska redogöras för i informationsförvaltningsplanen för informationens hela livscykel samt relateras till en process med en punktnotation för återsökning.

För att förbereda för e-arkivering kan processen se ut så här.