Riktlinje för hantering av personuppgifter.

Antagen av kommunstyrelsen:	2019-08-27 § 130
Ansvarig sektor:	Kommunstyrelsen
Ikraftträdande	2020-10-01
Giltighetstid	Gäller tills vidare
Revideras	Senast fyra år efter ikraftträdande
Diarienummer	KS.2019.204
Ansvarig handläggare	Administrativ chef, Kommunstyrelsen

Riktlinje för hantering av personuppgifter

Inledning och syfte

Följande riktlinje syftar till att konkretisera kommunens policy för hantering av personuppgifter samt ge vägledning och råd vid hantering av personuppgifter i Ale kommun.
Riktlinje som grundar sig på gällande lagar och förordningar, gäller samtliga nämnder i kommunen.

Organisatoriska och tekniska förutsättningar

Personuppgiftsansvar
Varje nämnd i Ale kommun är personuppgiftsansvariga för sina respektive verksamhetsområden.
Ansvaret innebär en skyldighet tillse att gällande lagstiftning efterlevs genom att bland annat:
• Fastställa ändamål och syfte med behandling av personuppgifter, innan behandling påbörjas
• Utse dataskyddsombud och svara för att vederbörande har förutsättningar och kunskap för att fullgöra sitt uppdrag.
• Säkerställa att det finns tekniska och organisatoriska förutsättningar att behandla personuppgifter med erforderlig säkerhet
• Kunna visa att kraven i lagstiftningen är uppfyllda
• Föra register över behandlingar av personuppgifter

Kommunstyrelsen har av fullmäktige givits ansvaret för att leda, samordna och ha uppsikt över kommunens arbete med att uppfylla gällande personuppgiftslagstiftning.

Dataskyddsombud
Den personuppgiftsansvarige ska utse ett dataskyddsombud.
Dataskyddsombudet ska anmälas till tillsynsmyndigheten.

Organisation
Varje personuppgiftsansvarig ska ha en person i verksamheten, en s.k. lokal personuppgiftskontakt, som är utsedd att vara kontaktperson i förhållande till dataskyddsombudet.
Kommunstyrelsens lokala personuppgiftskontakt ska ha en samordnande roll i förhållande till de övriga nämndernas lokala personuppgiftskontakter och också vara den centrala kontakten i förhållande till dataskyddsombudet.

Säkerhet
Behandling av personuppgifter får ske om lämplig teknisk och organisatorisk säkerhet vidtagits för behandlingen för att säkerställa en säkerhetsnivå utifrån lagens krav. Säkerheten ska baseras på erforderliga informationssäkerhetsklassningar och riskanalyser.
Vid planeringen av verksamheten ska särskild hänsyn tas till att personuppgifter inte behandlas i högre utsträckning, av fler personer än nödvändigt eller under

längre tid än vad som behövs. Anställda som kan komma att hantera personuppgifter ska också ges erforderlig information/utbildning kring personuppgiftshantering för att härigenom säkerställa att personuppgifter hanteras på ett lagligt och respektfullt sätt.

Incidentrapportering
Varje personuppgiftsansvarig ska kunna upptäcka, hantera och rapportera personuppgiftsincidenter som sker i den egna verksamheten.
Personsuppgiftsincident ska anmälas till tillsynsmyndigheten inom 72 timmar från det att överträdelsen upptäckts.
Varje personuppgiftsansvarig har ansvar för att rutin finns för att anmälan görs i tid och att incidenten i övrigt hanteras i enlighet med de krav som framgår av gällande lagstiftning.
Alla personuppgiftsincidenter ska anmälas och registreras centralt.

Kontroll över personuppgiftsbehandlingar

Register över behandlingar s.k. förteckning
Varje personuppgiftsansvarig ska föra ett register över behandling som utförs under dess ansvar.
Personuppgiftsbiträde och personuppgiftsbiträdesavtal
Den som behandlar personuppgifter på uppdrag av annan personuppgiftsansvarig blir personuppgiftsbiträde i förhållande till den personuppgiftsansvarige. Vid anlitandet av ett personuppgiftsbiträde ska säkerställas att vederbörande kan ge tillräckliga garantier om att upprätthålla lämplig teknisk och organisatorisk säkerhet i enlighet med gällande lagstiftning. Detta säkerställs genom ett personuppgiftsbiträdesavtal (s.k. PUB-avtal).
Varje personuppgiftsansvarig ska teckna ett PUB-avtal när vederbörande ger uppdrag till ett externt personuppgiftsbiträde att behandla personuppgifter.
Den personuppgiftsansvarige ska tillse att en förteckning över aktuella PUB-avtal och eventuella tillhörande underbiträdesavtal finns. Avtalen skall diarieföras i kommunens centrala ärendehanteringssystem.

Upphandling
Vid upphandlingar av produkter och tjänster ska särskilt utredas om användandet av det som inköpet avser eller annars som en följd av avtalsrelationen kan komma att leda till behandling av personuppgifter. Vid upphandlingar av produkter och tjänster som kan komma att leda till behandlingar av personuppgifter, ska krav ställas på alla utrustning lever upp till kraven i dataskyddsförordningen och annan nationell lagsstiftning inom dataskyddsområdet.
Vid utredning av vilka säkerhetskrav som bör ställas ska samråd ske med IT-avdelningen.

Registrerades rättigheter
Varje personuppgiftsansvarig ska ha rutiner för hur information tillhandahålls de registrerade.
Varje personuppgiftsansvarig ska ha rutiner för hanteringen av begäranden från de registrerade om att utöva sina rättigheter enligt gällande lagstiftning.