Reglemente för kommungemensamma behandlingar av personuppgifter

Antagen av:	Kommunfullmäktige 2018-06-13, § 58. Dnr KS 2018/66
Dokumentkategori:	Styrdokument
Dokumenttyp:	Reglemente

Innehållsförteckning

Bakgrund och syfte

Enligt artikel 28.3 dataskyddsförordningen ska personuppgiftsbiträdets hantering av personuppgifter regleras i avtal eller annan rättsakt (såsom i ett reglemente). Syftet är att säkerställa de registrerades fri- och rättigheter och att uppfylla artikel 28.3 Allmänna dataskyddsförordningen EU 2016/679, i det följande kallad dataskyddsförordningen. När personuppgiftsbiträdet finns utanför organisationen ska biträdesavtal tecknas och när personuppgiftsbiträdet finns inom organisationen ska hanteringen ske i enlighet med detta reglemente. Utöver reglementet ska den personuppgiftsansvarige lämna en instruktion till personuppgiftsbiträdet.

All behandling av personuppgifter inom Trosa kommun ska ske i enlighet med *Policy och riktlinje för behandling av personuppgifter i Trosa kommun.*

Personuppgiftsbiträde inom organisationen

När två eller flera nämnder i Trosa kommun hanterar personuppgifter gemensamt ska det anges vilken/vilka nämnder som är personuppgiftssansvariga för respektive behandling i *Förteckning över kommungemensam personuppgiftsbehandling*. Kommunkontoret ansvarar för att sammanställa förteckningen och den personuppgiftssansvarige ansvarar för att lämna information om nya behandlingar uppstår.

Den personuppgiftsansvarige ska lämna en instruktion till personuppgiftsbiträdet (den nämnd som behandlar personuppgifter för den personuppgiftsansvariges räkning) för varje enskild kommungemensam behandling. I instruktionen ska det tydliggöras vem/vilka som är personuppgiftsansvariga, vem/vilka som är personuppgiftsbiträden och hur personuppgiftsbiträdet får behandla personuppgifterna för den personuppgiftsansvariges räkning. Det ska även klargöras vilken integritetsnivå som ska uppnås vid respektive personuppgiftsbehandling.

Flera nämnder kan också vara gemensamt personuppgiftsansvariga det ska då tydliggöras vilket respektive ansvar nämnderna har för att fullgöra skyldigheterna enligt dataskyddsförordningen.

Definitioner

Behandling av personuppgifter	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.
Dataskyddslag	Avser sådan integritets- och personuppgiftslagstiftning samt all annan eventuell lagstiftning (inklusive förordningar och föreskrifter) som är tillämplig på den personuppgiftsbehandling som sker, inklusive nationell sådan lagstiftning och EU Lagstiftning, såsom denna kan komma att förändras över tid.
Personuppgiftsansvarig	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.
Gemensamt personuppgifts-ansvariga	När två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga.
Personuppgiftsbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.
Personuppgifter	Varje upplysning som avser en identifierad eller identifierbar fysisk person (registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska,

	fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.
Personuppgiftsincident	En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.
Registrerad	Den som personuppgiften avser.
Tredje land	En stat som inte ingår i Europeiska unionen eller är ansluten till Europeiska ekonomiska samarbetsområdet.

Behandling av personuppgifter

Behandlingen av personuppgifterna enligt instruktion

Personuppgiftsbiträdet får endast behandla den personuppgiftsansvariges personuppgifter i enlighet med den personuppgiftsansvariges skriftliga instruktioner för att fullgöra sitt uppdrag åt den personuppgiftsansvarige.

Personuppgiftsansvariges ansvar

Den personuppgiftsansvarige åtar sig att säkerställa att det finns en laglig grund för aktuella behandlingar och för att utforma skriftliga instruktioner till personuppgiftsbiträdet. Det krävs för att biträdet ska kunna fullgöra sitt uppdrag enligt detta reglemente.

Den personuppgiftsansvarige ska utan dröjsmål informera personuppgiftsbiträdet om förändringar i behandlingen vilka påverkar personuppgiftsbiträdets skyldigheter enligt gällande Dataskyddslag eller annan relevant lagstiftning.

Den personuppgiftsansvarige ansvarar för att informera registrerade om behandlingarna och för att, i de fall det krävs, inhämta samtycke från den registrerade samt tillvarata de registrerades rätt till insyn och radering m.m.

Personuppgiftsbiträdets ansvar

Personuppgiftsbiträdet förbinder sig att endast behandla personuppgifterna för de syften som anges i instruktionen och följa gällande Dataskyddslag eller annan relevant lagstiftning med avseende på behandling av personuppgifter och att hålla sig informerad om gällande rätt på området.

Personuppgiftsbiträdet ska vidta åtgärder för att skydda personuppgifterna mot förstörning, ändring, otillåten spridning och obehörig tillgång samt mot varje annat slag av otillåten behandling.

Personuppgiftsbiträdet åtar sig att säkerställa att samtliga personer som arbetar under dennes ledning följer vad som framgår av detta reglemente och gällande instruktion från personuppgiftsansvarig, samt informeras om relevant lagstiftning.

Personuppgiftsbiträdet ska vid behov assistera personuppgiftsansvarig med att ta fram information som begärts av tredje man.

Om personuppgiftsbiträdet anser att personuppgiftsansvarigas instruktioner är otydliga, olagliga eller saknas och personuppgiftsbiträdet bedömer dem som nödvändiga för att genomföra sina åtaganden ska personuppgiftsbiträdet utan dröjsmål informera personuppgiftsansvarig om detta och invänta nya instruktioner.

Säkerhetsåtgärder
Personuppgiftsbiträdet åtar sig att vidta alla lämpliga tekniska och organisatoriska säkerhetsåtgärder i enlighet med gällande dataskyddslagstiftning samt de eventuella åtgärder som framgår av instruktionerna för att skydda personuppgifterna.

I det fall personuppgiftsbiträdet behandlar känsliga personuppgifter vilka omfattas av sekretess, ställs särskilt höga säkerhetskrav. Personuppgiftsansvarig får då lämna ytterligare instruktioner om säkerhetsåtgärder.
Personuppgiftsbiträdet ska ha ett behörighetskontrollsystem som förhindrar obehörig behandling av personuppgifter eller obehörig åtkomst till personuppgifter. Personuppgiftsbiträdet ska använda ett loggsystem som möjliggör att behandling av personuppgifter kan spåras och ska även se till att loggarna har ett adekvat säkerhetsskydd.

Personuppgiftsbiträdet ska genom behörighetskontrollsystemet aktivt begränsa åtkomsten till personuppgifterna till sådana personer som arbetar under dennes ledning och som behöver personuppgifterna för att utföra sina arbetsuppgifter.

Personuppgiftsbiträdet ska utan dröjsmål underrätta personuppgiftsansvarig om eventuella kontakter med tillsynsmyndighet som rör eller kan vara av betydelse för behandling av personuppgifterna.

Sekretess
Personuppgiftsbiträdet ska vid behandling av personuppgifter säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.

Personuppgiftsincident
Upptäcks en personuppgiftsincident ska den som upptäcker incidenten (personuppgiftsansvarig/personuppgiftsbiträde) handla efter gällande rutin för personuppgiftsincidenter.

Tredje land
Personuppgiftsbiträdet får endast överföra personuppgifter till tredje land, för exempelvis service, support, underhåll, utveckling, drift eller liknande hantering, om den personuppgiftsansvarige skriftligt godkänt sådan överföring och utfärdat särskilda instruktioner.

Gemensamt personuppgiftsansvariga

Gemensamt personuppgiftsansvariga ska skriftligen fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt dataskyddsförordningen. Särskilt ska det tydliggöras vad som gäller vid utövandet av den registrerades rättigheter och de ansvarigas respektive skyldigheter att tillhandahålla information till den registrerade när personuppgifter samlas in.