Policy och riktlinje för hantering av personuppgifter i Trosa kommun

Antagen av:	Kommunfullmäktige 2018-04-25, § 36, dnr KS 2018/65
Dokumentkategori:	Styrdokument
Dokumenttyp:	Policy

Innehållsförteckning

Policy för hantering av personuppgifter i Trosa kommun

- Varje behandling av personuppgifter ska ske med hänsyn till den enskildes personliga integritet och rättigheter

- Varje behandling av personuppgifter ska ske i enlighet med gällande lagstiftning

- Vid behandling av personuppgifter ska följande grundläggande principer tillämpas:

  – Behandlingen ska vara laglig, korrekt och öppen gentemot den registrerade.

  – Innan behandling påbörjas ska ett särskilt och uttryckligt angivet samt berättigat ändamål med behandlingen vara fastställt (ändamålsbegränsning). Hantering utöver detta ändamål kan vara otillåtet då det kan vara oförenligt med det ursprungliga ändamålet.

  – Endast de uppgifter som är adekvata och relevanta för ändamålet får samlas in och insamlingen får inte vara mer omfattande än nödvändigt (uppgiftsminimering).

  – Insamlade personuppgifter ska vara korrekta och uppdaterade.

  – Insamlade personuppgifter får bara bevaras i identifierbar form så länge det är nödvändigt för ändamålet (lagringsminimering).

  – Lämpliga tekniska och organisatoriska åtgärder baserade på informationssäkerhetsklassningar och riskanalyser ska skydda personuppgifterna (integritet och konfidentialitet).

  – Endast behöriga ska få åtkomst till personuppgifter (åtkomstbegränsning).

  – Den personuppgiftsansvarige ska kunna visa att behandlingen sker med följsamhet till principerna i dataskyddsförordningen.

  – Varje nämnd och bolag i kommunen ska utse ett dataskyddsombud.

  – Vid varje behandling av personuppgifter ska ett sådant förhållningssätt iakttas att risken för skada för den registrerade minimeras.

Riktlinje för hantering av personuppgifter i Trosa kommun

Inledning

Följande riktlinje syftar till att konkretisera policyn samt ge vägledning och råd vid hantering av personuppgifter i Trosa kommun inklusive dess bolag.
Riktlinjen som grundar sig på bestämmelserna i lagstiftningen kan komma att justeras vid förändringar av gällande rätt.

Omfattning

Denna riktlinje gäller för Trosa kommuns samtliga nämnder samt styrelser i de kommunala bolagen.

Bakgrund

Från och med den 25 maj 2018 gäller EU:s dataskyddsförordning (679/2016) för hantering av personuppgifter. Förordningen ersätter personuppgiftslagen, PuL (1998:204). Förordningen behöver inte implementeras i svensk rätt genom svensk lag utan är direkt tillämplig.
Det är av stor vikt att fysiska personer har kontroll över sina egna personuppgifter. Målet med dataskyddsförordningen anges vara att stärka och harmonisera den rättsliga säkerheten och smidigheten för fysiska personer, ekonomiska operatörer och myndigheter i unionen.

Övergångsregler

All pågående behandling ska vara anpassad till förordningen den 25 maj 2018. Om pågående behandling grundar sig på samtycke enligt direktiv 95/46/EG, är det inte nödvändigt att den registrerade på nytt ger sitt samtycke för att den personuppgiftsansvarige ska kunna fortsätta med behandlingen i fråga efter det att denna förordning börjar tillämpas, om det sätt på vilket samtycket gavs överensstämmer med villkoren i denna förordning. Beslut av kommissionen som antagits och tillstånd från tillsynsmyndigheterna som utfärdats på grundval av direktiv 95/46/EG ska fortsatt vara giltiga tills de ändras, ersätts eller upphävs.

Materiellt tillämpningsområde

Förordningen ska tillämpas på all hantering av personuppgifter som helt eller delvis företas på automatisk väg samt på annan än automatisk behandling av personuppgifter som ingår eller kommer att ingå i ett register. Med ett register avses en strukturerad samling uppgifter som är tillgängliga för sökning eller sammanställda enligt särskilda kriterier.

Personuppgiftsansvar

Trosa kommuns samtliga nämnder samt styrelser i de kommunala bolagen, är personuppgiftsansvariga för sina respektive verksamhetsområden. Ansvaret innebär en yttersta skyldighet att se till att gällande lagstiftning följs genom att bland annat:

- fastställa ändamål och syfte med behandling av personuppgifter innan behandling påbörjas,
- utse dataskyddsombud och svara för att denne har förutsättningar och nödvändig kunskap för att fullgöra sitt uppdrag,
- säkerställa att det finns tekniska och organisatoriska förutsättningar att behandla personuppgifter med lämplig säkerhet,
- kunna visa att kraven i lagstiftningen är uppfyllda genom noggrann dokumentation samt verifierande tester,
- föra register över behandlingar av personuppgifter.

Laglig behandling av personuppgifter

Personuppgifter får endast behandlas om det finns laglig grund för behandlingen. Den lagliga grunden ska fastställas innan behandling påbörjas enligt någon av punkterna:

- Samtycke (ska vara informerat, frivilligt och specifikt samt kunna visas).
- Behandlingen är nödvändig för att fullgöra ett avtal.
- Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som den personuppgiftsansvarige har.
- Behandlingen är nödvändig för att skydda ett grundläggande intresse för den registrerade eller annan fysisk person.
- Behandlingen är nödvändig för utföra uppgift av allmänt intresse.
- Behandlingen är nödvändig att utföra som ett led i den personuppgiftsansvariges myndighetsutövning.

Innan behandling av personuppgifter

Innan behandling av personuppgifter påbörjas krävs följande:

1. Dokumentera ändamål och syfte samt under hur lång tid behandlingen beräknas pågå.
2. Fastställ rättslig grund.
3. Inhämta samtycke vid behov.
4. Säkerställ att behandlingen sker i enlighet med de grundläggande principerna och denna policy och riktlinje.
5. Vid behov, rådgör med dataskyddsombudet.
6. Klassificera personuppgifterna utifrån kommunens informationssäkerhetsnivåer. Om klassningen hamnar på *mycket hög nivå* eller *hög nivå* ska en riskanalys genomföras.
7. Samråd med dataskyddsombudet om konsekvensanalys behöver utföras när riskanalysen hamnar på rött. Konsekvensanalys ska alltid utföras vid behandling som tas upp i dataskyddsförordningens artikel 35 p 3.

8. Samråd med tillsynsmyndighet om hög risk inte kan åtgärdas inför behandling av personuppgifter.
9. Se till att det finns tillräckliga tekniska och organisatoriska säkerhetsåtgärder utifrån genomförd informationssäkerhetsklassning och resultat från eventuell riskanalys och konsekvensanalys.
10. Klargör om, och i så fall vilken, kommunikation med den registrerade som är nödvändig.
11. Upprätta personuppgiftsbiträdesavtal vid behov.
12. Meddela personuppgiftsambassadören hos den personuppgiftsansvarige om den nya behandlingen. Den nya behandlingen ska läggas till i det register som förs över behandlingar av personuppgifter.

Säkerhet

Behandling av personuppgifter får ske om lämplig teknisk och organisatorisk säkerhet vidtagits för behandlingen. Säkerheten ska baseras på genomförda informationssäkerhetsklassningar och riskanalyser.

Säkerhet utgörs av inbyggt dataskydd och dataskydd som standard vilket för personuppgiftshanteringen bl.a. innebär att:

- säkerställandet av personuppgiftshanteringen ska finnas med redan från den initiala planeringen och täcka såväl tekniska som organisatoriska åtgärder,
- nyttja åtgärder som uppgiftsminimering, lagringsminimering, fritextfältsmimimering och åtkomstbegränsning.

Säkerhet utgörs även av införande och tillämpning av rutiner för att:

- kontinuerligt testa, undersöka och visa på effektiviteten av införda säkerhetsåtgärder,
- anmäla personuppgiftsincident till tillsynsmyndighet,
- vid behov kunna ge incidentinformation till berörda registrerade,
- vid behov kunna involvera och rådgöra med dataskyddsombudet.

Register över behandling

Varje personuppgiftsansvarig ska föra ett register över behandling som utförs under dess ansvar. Registret ska minst innehålla:

- Namn och kontaktuppgifter till den personuppgiftsansvarige samt Dataskyddsombudet.
- Ändamålet med behandlingen.
- Kategori av registrerade och personuppgifter.
- Mottagare av personuppgifter, i förekommande fall.
- Eventuell överföring till tredje land med tillhörande säkerhetsåtgärder.
- Uppskattad tidsfrist för radering.
- Beskrivning av tekniska och organisatoriska säkerhetsåtgärder för behandlingen om inte detta hindras av exempelvis sekretessbestämmelser.

Personuppgiftsbiträde

Den som behandlar personuppgifter på uppdrag av annan personuppgiftsansvarig blir personuppgiftsbiträde i förhållande till den personuppgiftsansvarige. Vid anlitandet av ett personuppgiftsbiträde ska det säkerställas att denne kan ge tillräckliga garantier om att upprätthålla lämplig teknisk och organisatorisk säkerhet i enlighet med gällande rätt.

Personuppgiftsbiträdesavtal

Personuppgiftsbiträdets (biträdet) behandling av personuppgifter ska regleras av personuppgiftsbiträdesavtal mellan biträdet och den personuppgiftsansvarige (ansvarige).

I avtalet ska följande anges:

- Vem som är personuppgiftsansvarig respektive personuppgiftsbiträde.
- Vad behandlingen avser, dess varaktighet, art, ändamål, typ av personuppgifter samt kategori av registrerade.
- Den ansvariges skyldigheter och rättigheter.
- Att biträdet endast får behandla personuppgifter i enlighet med den ansvariges instruktion.
- Att biträdet iakttar erforderlig konfidentialitet och tystnadsplikt.
- Att biträdet vidtar alla lämpliga tekniska och organisatoriska åtgärder för att säkerställa adekvat skydd för personuppgifterna samt att detta kan visas genom att ge ansvarige tillgång till vederbörlig information.
- Att biträdet ska bistå den ansvarige i att uppfylla sina förpliktelser enligt förordningen.
- Att biträdet inte får anlita underleverantör för behandling av den ansvariges personuppgifter utan den ansvariges skriftliga medgivande till detta. Om biträdet anlitar underleverantör ska personuppgiftsbiträdesavtal upprättas även mellan dessa parter.
- Att överföring till tredje land inte får ske utan att adekvata säkerhetsåtgärder är uppfyllda.
- Reglering om inom vilken tid radering eller överflyttning av personuppgifter sker vid avtals upphörande.

Kommunens gemensamma behandlingar

Kommunens gemensamma personuppgiftsbehandlingar regleras i *Reglemente för kommungemensamma behandlingar av personuppgifter.*

Dataskyddsombud

Den personuppgiftsansvarige ska utse ett dataskyddsombud att representera den ansvariges verksamhet. Det kan vara en person för flera verksamheter och det kan vara en anställd eller extern aktör. Dataskyddsombudet ska utses på grundval av sina yrkesmässiga kvalifikationer och i synnerhet sakkunskap om lagstiftning och praxis avseende dataskydd. Dataskyddsombudet ska anmälas till tillsynsmyndigheten.

Dataskyddsombudet ska minst ha följande uppgifter:

- Informera och ge råd till den personuppgiftsansvarige och anställda om skyldigheterna enligt dataskyddsförordningen.
- Övervaka efterlevnad av förordningen avseende fungerande rutiner och åtgärder, ansvarstilldelning, information, utbildning och granskning.
- Ge råd vid konsekvensbedömningar.
- Samarbeta med tillsynsmyndigheten.
- Vara kontaktpunkt för tillsynsmyndigheten i alla frågor som rör behandling av personuppgifter.
- Vara kontaktperson till den registrerade.
- Delta i frågor som rör skyddet av personuppgifter.
- Får även ha andra uppgifter om det inte leder till intressekonflikt.

Den personuppgiftsansvarige ska säkerställa att dataskyddsombudet:

- på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter,
- tillhandahålls de resurser och det stöd som krävs för att fullgöra sina uppgifter,
- upprätthåller sin sakkunskap,
- inte blir föremål för sanktioner eller avsätts på grund av att ombudet utför sitt uppdrag,
- inte bli föremål för otillbörlig påverkan i utövande av sitt uppdrag,
- rapporterar direkt till den personuppgiftsansvarige eller dennes högsta förvaltningsnivå.