Riktlinjer för dataskydd

Inledning

Följande riktlinje syftar till att konkretisera policyn för dataskydd samt ge vägledning och råd vid hantering av personuppgifter i X kommun.

Riktlinjen, som grundar sig på bestämmelserna i lagstiftningen och kan komma att justeras vid förändringar av gällande rätt ska även förtydliga ansvarsförhållanden angående personuppgiftshantering.

Omfattning

Denna riktlinje gäller för X kommuns samtliga nämnder samt styrelser i sådana organisationer där X kommun har det rättsligt bestämmande inflytandet. Riktlinjen avser 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.

Bakgrund

Från och med den 25 maj 2018 gäller EU:s dataskyddsförordning (679/2016) för hantering av personuppgifter. Dataskyddsförordningen (GDPR) ersätter personuppgiftslagen, PuL (1998:204). Förordningen behöver inte implementeras i svensk rätt genom svensk lag utan är direkt tillämplig.

I Sverige finns kompletterande bestämmelser i lag 2018:218 med kompletterande bestämmelser till EU:s dataskyddsförordning (kompletteringslagen) och även en svensk förordning med kompletterande bestämmelser till EU:s dataskyddsförordning, 2018:2019. Därutöver finns också särskilda registerförfattningar.

Det är av stor vikt att fysiska personer har kontroll över sina egna personuppgifter. Syftet med GDPR är att skydda enskilda personer vad gäller behandlingen av deras personuppgifter, men också att säkerställa fritt flöde av personuppgifter inom EU.

För att kunna följa lagen på ett effektivt sätt måste kommunen skapa rutiner och tydliggöra ansvarsförhållanden kring hantering av personuppgifter. De befattningar i kommunen som behandlar personuppgifter ska på ett hållbart sätt stödjas med både kompetens och resurser för att efterleva lagen. När privatpersoner utövar sina rättigheter enligt dataskyddsförordningen ska kommunens berörda personal agera på ett effektivt och lagligt sätt genom att agera utifrån väl utvecklade rutiner.

Personuppgiftsansvar

X kommuns samtliga nämnder samt styrelser i sådana organisationer där X kommun har det rättsligt bestämmande inflytandet, är personuppgiftsansvariga för sina respektive verksamhetsområden. Ansvaret innebär en yttersta skyldighet att tillse att gällande lagstiftning efterlevs genom att bl.a.

- Fastställa ändamål och syfte med behandling av personuppgifter, innan behandling påbörjas
- Utse dataskyddsombud
- Säkerställa att det finns tekniska och organisatoriska förutsättningar att behandla personuppgifter med erforderlig säkerhet
- Kunna visa att kraven i lagstiftningen är uppfyllda genom noggrann dokumentation samt verifierande tester
- Föra register över behandlingar av personuppgifter

Laglig grund för behandling av personuppgifter
Personuppgifter får endast behandlas om det finns laglig grund för behandlingen. Den lagliga grunden enligt art 6 GDPR ska fastställas innan behandling påbörjas enligt någon av nedan punkter:

a. Samtycke – ska vara informerat, frivilligt och specifikt samt kunna visas.
b. Behandlingen är nödvändig för att fullgöra ett avtal eller vidta åtgärder på begäran av den registrerade inför ett avtal
c. Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som den personuppgiftsansvarige har
d. Behandlingen är nödvändig för att skydda ett grundläggande intresse för den registrerade eller annan fysisk person
e. Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning
f. Berättigat intresse – ska ej användas av myndigheter

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 kommunens policy och riktlinje för dataskydd
5. Vid behov, rådgör med dataskyddsombudet
6. Klassificera personuppgifterna utifrån informationssäkerhetsnivå och genomföra en riskanalys av den planerade behandlingen. Dataskyddsombudet ska involveras i riskanalysen.
7. Samråd med tillsynsmyndigheten om hög risk inte kan åtgärdas inför behandling av personuppgifter
8. Se till att det finns tillräckliga tekniska och organisatoriska säkerhetsåtgärder utifrån genomförd informationssäkerhetsklassning och resultat från riskanalys
9. Klargör om, och i så fall vilken, kommunikation med den registrerade som är nödvändigt
10. Upprätta personuppgiftsbiträdesavtal vid behov
11. Anteckna ny behandling av personuppgifter i registerförteckningen över personuppgiftsbehandlingar

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
  - säkerställa att kommunens grundsäkerhetsnivå för informationssäkerhet (nivå 1) föreligger samt om möjligt nyttja åtgärder som pseudonymisering, anonymisering eller kryptering

- säkerställa att kommunens förhöjda säkerhetsnivå (nivå 2) för informationssäkerhet föreligger avseende särskilda personuppgifters konfidentialitet och riktighet vilket för elektronisk hantering bl.a. innebär nyttjande av kryptering samt stark autentisering motsvarande tillitsnivå 3 för e-legitimation
- nyttja åtgärder som uppgiftsminimering, lagringsminimering, fritextfältsminimering och åtkomstbegränsning

- 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

Personuppgiftsbiträde
Den som behandlar personuppgifter på uppdrag av annan personuppgiftsansvarig blir personuppgiftsbiträde i förhållande till den personuppgiftsansvarige. Vid anlitandet av ett personuppgiftsbiträde ska 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).

X kommun bör använda senaste versionen av den personuppgiftsbiträdes-avtalsmallen som kommunalförbundet Sydarkivera rekommenderar. Av avtalet ska bland annat framgå:

- Vem 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.

Register över behandling
Varje personuppgiftsansvarig ska enligt art 30 GDPR föra ett register över behandling som utförs under dess ansvar. Registret bör minst innehålla:

- Kontaktuppgifter till personuppgiftsansvarig och dataskyddsombudet
- Namn eller beskrivning på behandlingen
- Beskrivning av ändamålet med behandlingen
- Kategori av registrerade personer
- Typer av personuppgifter som förekommer i behandlingen
- 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
- Vilken laglig grund behandlingen har
- Vilket system som behandlingen ingår i
- Finns personuppgiftsbiträdesavtal bör uppgift om detta framgå

Dataskyddsombud
Den personuppgiftsansvarige ska utse ett dataskyddsombud och anmäla det till tillsynsmyndigheten Datainspektionen.

X kommun är ansluten till tjänsten gemensamt dataskyddsombud som utförs av en grupp, dataskyddsteamet, inom kommunalförbundet Sydarkivera. Enligt avtal om anslutande tjänst för medlemmar i Sydarkivera har dataskyddsteamet följande uppgifter:

- Informera och ge råd till den personuppgiftsansvarige och anställda om skyldigheterna enligt dataskyddsförordningen och annan dataskyddslagstiftning.
- Planera och genomföra utbildningar i dataskyddsförordningen och annan dataskyddslagstiftning hos anslutna medlemmar
- Ta fram mallar för interna riktlinjer och styrdokument
- Ge råd och stöd vad gäller risk- och sårbarhetsanalyser och konsekvensbedömningar vad gäller dataskydd
- Vara kontaktperson mot Datainspektionen och samarbeta på olika sätt med tillsynsmyndigheten.
- Ge råd och stöd vid upphandling av nya system eller applikationer
- Ta fram mallar för personuppgiftsbiträdesavtal
- Övervaka efterlevnaden av dataskyddsförordningen hos personuppgiftsansvarig

Enligt avtal om anslutande tjänst ska den personuppgiftsansvarige ska

- Utse en kontaktperson som leder det lokala dataskyddsarbetet som är kontaktperson gentemot dataskyddsombudet
- Fastställa en lokalt anpassad organisation för dataskyddsarbetet med råd och stöd från dataskyddsombudet
- Kontaktpersonen är den som enligt avtalet ska rapportera till kommun- och förvaltningsledning. Normalt är annars att det är dataskyddsombudet som rapporterar, men av praktiska och effektivitetsskäl är det kontaktpersonen som avrapporterar. Avrapporteringen bör ske i samråd med dataskyddsombudet.
- Fastställa interna riktlinjer och policydokument för behandling av personuppgifter samt andra dokument som rör behandling av personuppgifter med råd och stöd från dataskyddsombudet.

Bilaga 1: Informationsklassningsnivåer

Konfidentialitet - att informationen kan åtkomstbegränsas.
Riktighet – att information ska vara tillförlitlig, korrekt och fullständig.
Tillgänglighet – att information ska kunna nyttjas efter behov, i förväntad utsträckning samt av rätt person med rätt behörighet.
Spårbarhet – att specifika aktiviteter som rör informationen kan spåras.

Nivå 0 – Ingen eller försumbar skada

- Inga svårigheter för verksamheten att nå målen.
- Ingen eller endast försumbar påverkan på samhällsviktiga funktioner vid egen eller annan organisation

Nivå 1 – Måttlig skada

- Inga märkbara större svårigheter för verksamheten att nå målen.
- Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation.
- Enskilda individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan.

Nivå 2 – Betydande skada

- Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder).
- Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Samhällsviktiga funktioner i egen eller annan organisation påverkas troligen inte.
- Enskilda individer kan uppleva konsekvenser, såsom stora besvär eller stor ekonomisk påverkan, av störningen.

Nivå 3 – Allvarlig skada

- Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen.
- Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt.
- Individers liv och hälsa äventyras

Nivå 4 – Synnerligen allvarlig

- Röjande av informationen medför **skada för rikets säkerhet som inte endast är ringa.**
- Systemet behandlar information som omfattas av sekretess och rör rikets säkerhet (hemliga uppgifter) där röjande av information kan ge oöverskådliga konsekvenser där t ex omfattande fara för liv och hälsa föreligger.
- Informationen omfattas av t ex säkerhetsskyddslagstiftningen