Oskarshamns kommun

Styrande dokument

Riktlinjer för dataskydd

Fastställd av Kommunstyrelsen

Senast reviderad av 2018-05-17

Gäller från och med 2018-05-25

Innehållsförteckning

1 Inledning

Följande riktlinje syftar till att konkretisera dataskyddspolicyn samt ge vägledning och råd vid hantering av personuppgifter i Oskarshamns 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

2 Omfattning

Denna riktlinje gäller för Oskarshamns kommuns samtliga nämnder samt styrelser i sådana organisationer där Oskarshamns kommun har det rättsligt bestämmande inflytande. 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.

3 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.

Genom den nya lagstiftningen ska den tillit som behövs för att utveckla den digitala ekonomin över hela den inre marknaden uppnås. 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.

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.

4 Personuppgiftsansvar

Oskarshamns kommuns samtliga nämnder samt styrelser i sådana organisationer där Oskarshamns 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 och svara för att denne har förutsättningar och besitter erforderlig kunskap och 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 genom noggrann dokumentation samt verifierande tester
- Föra register över behandlingar av personuppgifter

5 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 nedan punkter:

- 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 att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning
- Samtycke – ska vara informerat, frivilligt och specifikt samt kunna visas.

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 tillsynsmyndighet 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. Se till att dataskyddsombudet godkänner behandlingen
12. Anteckna ny behandling av personuppgifter i registerförteckningen över personuppgiftsbehandlingar

6 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

7 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.

8 Personuppgiftsbiträdesavtal

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

- Vem som är personuppgiftsansvarigt, 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.

9 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, personuppgifter samt behandlingar
- 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

10 Dataskyddsombud

Den personuppgiftsansvarige ska utse ett Dataskyddsombud att representera den ansvariges verksamhet. 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 riskanalysen
- Samarbeta med tillsynsmyndigheten
- Vara kontaktpunkt för tillsynsmyndigheten i alla frågor som rör behandling av personuppgifter
- Delta i frågor som rör skyddet av personuppgifter

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

- 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