RIKTLINJE

Riktlinjer för dataskydd

2019

RLSHAMN

Innehåll

1. Inledning

Från och med den 25 maj 2018 gäller EU:s allmänna dataskyddsförordning (679/2016) (GDPR) för behandling av personuppgifter. Kompletterande bestämmelser finns i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning. Därutöver finns det särskilda registerförfattningar.

Riktlinjerna, som grundar sig på bestämmelserna i dataskyddsförordningen och kompletterande svensk lagstiftning, kan komma att justeras vid förändringar av gällande rätt.

Riktlinjerna gäller för anställda och förtroendevalda i Karlshamns kommuns nämnder.

Riktlinjerna avser behandling 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.

1.1 Syfte

Riktlinjerna syftar till att konkretisera dataskyddspolicyn och ge en beskrivning av hur personuppgifter ska behandlas i Karlshamns kommun. Riktlinjerna ska även tydliggöra ansvarsförhållandena avseende behandling av personuppgifter i Karlshamns kommun.

Dataskyddsförordningens syfte är att fysiska personer ska ha kontroll över sina egna personuppgifter. För att kunna följa lagen på ett effektivt sätt måste kommunen skapa rutiner och tydliggöra ansvarsförhållandena kring behandling av personuppgifter. De befattningshavare i kommunen som behandlar personuppgifter ska på ett hållbart sätt stödjas med både kompetens och resurser för att efterleva lagstiftningen.

1.2 Definitioner

Med ***personuppgift*** avses varje upplysning som avser en identifierad eller identifierbar fysisk person. Med identifierbar avses en fysisk person som direkt eller indirekt kan identifieras med hjälp av en identifierare som t.ex. ett namn, ett identifikationsnummer (t.ex. personnummer, kundnummer), en lokaliseringsuppgift (t.ex. GPS-information) eller onlineidentifikatorer (t.ex. IP-nummer) eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Med ***behandling*** avses en åtgärd eller en kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej. Exempel på behandlingar är insamling, registrering, lagring, läsning, användning, utlämning genom överföring, radering och förstöring.

1.3 Personuppgiftsansvar

Karlshamns kommuns nämnder är personuppgiftsansvariga för de personuppgifter som behandlas inom nämndernas respektive verksamhetsområden. Kommunstyrelsen är även personuppgiftsansvarig för de typer av personuppgiftsbehandlingar som är gemensamma för hela kommunen enligt vad som angivits i kommunstyrelsens registerförteckning samt för den behandling av personuppgifter som sker i kommunfullmäktige och hos kommunfullmäktigeberedningar.

Den som är personuppgiftsansvarig har en yttersta skyldighet att tillse att gällande lagstiftning efterlevs.

1.4 Dataskyddsombud

Alla Karlshamns kommuns nämnder är skyldiga att utse ett dataskyddsombud och anmäla det till tillsynsmyndigheten Datainspektionen. Därför är Karlshamns kommun ansluten till tjänsten gemensamt dataskyddsombud som utförs av en grupp, dataskyddsteamet, inom kommunalförbundet Sydarkivera.

Sydarkivera ska:

- Informera och ge råd till de personuppgiftsansvariga nämnderna och dess anställda om skyldigheter enligt dataskyddsförordningen och annan dataskyddslagstiftning.
- Planera och genomföra utbildningar i dataskyddsförordningen och annan dataskyddslagstiftning hos anslutna förbundsmedlemmar.
- Ta fram mallar för interna riktlinjer och policydokument för behandling av personuppgifter hos den personuppgiftsansvarige, t ex inventeringsrutiner, incidenthantering och informationsrutiner till registrerade.
- Samarbeta med och vara kontaktperson för Datainspektionen.
- Ge råd vad gäller risk- och konsekvensbedömningar avseende dataskydd.
- Ge råd vid upphandling av system/applikationer som rör personuppgifter.
- Ta fram mallar för avtal med personuppgiftsbiträden.
- Övervaka efterlevnaden av dataskyddsförordningen och annan dataskyddslagstiftning hos den personuppgiftsansvarige.
- Följa rättsutvecklingen inom området för dataskydd och delta i nätverk och projekt för att upprätthålla hög kompetens.

Kommunen ska:

- Utse en kontaktperson för dataskyddsfrågor som leder det lokala dataskyddsarbete och som är kontaktperson gentemot dataskyddsombudet. I Karlshamns kommun är kommunjurist utsedd till kontaktperson.
- Fastställa en lokalt anpassad organisation för dataskyddsarbetet med råd och stöd från dataskyddsombudet.
- Fastställa interna riktlinjer och policydokument för behandling av personuppgifter samt andra dokument som rör behandling av personuppgifter med råd och stöd från dataskyddsombudet.

2. Laglig grund för behandling av personuppgifter

Personuppgifter får endast behandlas om det finns laglig grund för behandlingen. Vilken laglig grund som är tillämplig för behandlingen ska fastställas innan behandlingen påbörjas. De lagliga grunderna är:

- för att fullgöra en rättslig förpliktelse,
- för att utföra en uppgift av allmänt intresse,
- som ett led i myndighetsutövning,
- för att fullgöra ett ingånget avtal eller ingå ett avtal,
- på grund av ett grundläggande intresse,
- när samtycke från den registrerade finns, eller
- när det finns ett berättigat intresse. Behandling på grund av berättigat intresse får dock inte användas av myndigheter när de fullgör sina uppgifter.

Observera att myndigheter har begränsade möjligheter att använda sig av samtycke som laglig grund. Samtycke ska lämnas frivilligt och under jämlika maktförhållanden. Eftersom maktförhållandet ofta är ojämlikt i relationen mellan kommun och medborgare kan samtycke användas av kommunen endast i begränsad utsträckning. Samtycke ska inte användas när någon annan laglig grund är tillämplig.

2.1 Känsliga personuppgifter

Enligt dataskyddsförordningen gäller särskilda bestämmelser för vissa kategorier av personuppgifter, s.k. känsliga personuppgifter. Till känsliga personuppgifter räknas personuppgifter som avslöjar ras[1] eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Behandling av känsliga personuppgifter är som utgångspunkt inte tillåten. För att kommunen ska kunna behandla sådana uppgifter krävs därför att något undantag är tillämpligt. Exempel på undantag som kan vara tillämpliga i Karlshamns kommuns verksamheter är:

- för att efterleva offentlighetsprincipen, t.ex. i hanteringen av allmänna handlingar,
- för att kunna handlägga ärenden, eller
- i annat fall, om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

2.2 Extra skyddsvärda personuppgifter

Utöver känsliga personuppgifter finns extra skyddsvärda personuppgifter, även kallade integritetskänsliga personuppgifter. Det kan till exempel vara

- löneuppgifter
- uppgifter om lagöverträdelser
- värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler
- information som rör någons privata sfär
- uppgifter om sociala förhållanden.

Samma krav på laglig grund gäller för integritetskänsliga uppgifter som för andra personuppgifter som inte är känsliga personuppgifter. Integritetskänsliga uppgifter medför dock krav på en högre säkerhetsnivå än för andra uppgifter och kan vara avgörande för om en personuppgiftsincident måste anmälas till Datainspektionen. Att integritetskänsliga uppgifter förekommer bör också ha betydelse för riskbedömningen när konsekvensanalys genomförs.

2.3 Personnummer och samordningsnummer

Personnummer och samordningsnummer får behandlas utan samtycke från den registrerade endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. En omständighet av betydelse som ska vägas in vid intresseavvägningen är exempelvis om det eftersträvade syftet med behandlingen kan uppnås på annat sätt.

3. Säkerhet

Behandling av personuppgifter får ske när lämplig teknisk och organisatorisk säkerhet säkerställts för behandlingen. Säkerheten ska baseras på genomförda riskanalyser och eventuella konsekvensbedömningar. Lämpliga säkerhetsåtgärder ska vidtas med beaktande av behandlingens art, omfattning, sammanhang och ändamål jämfört den risk som bedöms finnas för de registrerades rättigheter och friheter. I bedömningen av risken ska särskild hänsyn tas till sannolikheten för oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till personuppgifterna.

Lämpliga säkerhetsåtgärder kan vara till exempel:

- pseudonymisering och kryptering av personuppgifter,

[1] I svensk lagstiftning används inte begreppet ras. I dataskyddsförordningen används dock begreppet, varför det är återgivet här.

- tekniska lösningar och rutiner för att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,
- tekniska lösningar och rutiner för att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,
- införande av rutiner för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet, och/eller
- införande av rutiner för hantering av personuppgiftsincidenter, inklusive anmälan till Datainspektionen och uppföljning.

Det åligger den personuppgiftsansvarige att tillse att de personer som utför arbete under den personuppgifts-ansvariges överinseende och i samband med det kommer i kontakt med personuppgifter behandlar dessa endast i enlighet med instruktion från den personuppgiftsansvarige.

4. Riskarbete

Om en behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska en konsekvensbedömning utföras. Syftet är att säkerställa att gällande dataskyddsreglering efterlevs, samt att genom dokumentation kunna visa Datainspektionen att så är fallet.

4.1 Riskanalys

Innan en konsekvensbedömning görs ska en riskanalys genomföras. Riskanalysen tjänar till att utreda huruvida en konsekvensbedömning behövs. Det ska vara en kartläggning av vilka risker en behandling av personuppgifter kan innebära, sannolikheten att risken inträffar och förslag till lämpliga säkerhetsåtgärder. Riskanalysen ska dokumenteras. Om riskanalysen visar att en konsekvensbedömning bör göras, eller om riskanalysen visar att det rör sig om ett gränsfall, ska en konsekvensbedömning utföras.

4.2 Konsekvensbedömning

Konsekvensbedömningen ska som utgångspunkt utföras innan en behandling påbörjas. En genomförd konsekvensbedömning kan dock behöva omprövas och uppdateras kontinuerligt, t.ex. på grund av förändrade tekniska eller organisatoriska förutsättningar. En enda bedömning får omfatta en serie liknande behandlingar som medför liknande höga risker.

Vid genomförande av en konsekvensbedömning avseende dataskydd ska dataskyddsombudet, Sydarkivera, rådfrågas.

En konsekvensbedömning ska enligt förordningen göras vid:

- Automatiskt beslutsfattande som grundar sig på en systematisk och omfattande bedömning av människors personliga aspekter, till exempel profilering.
- Behandling i stor omfattning av känsliga personuppgifter eller av personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott,
- Systematisk övervakning av en allmän plats i stor omfattning.

Utöver i dessa situationer har Datainspektionen har tagit fram en förteckning över när en konsekvensbedömning ska göras. Om två eller flera av kriterierna i förteckningen nedan är uppfyllda behöver en konsekvensbedömning sannolikt göras. Så snart en punkt är uppfylld ska en konsekvensbedömning alltid övervägas. Observera att listan inte är uttömmande. Det kan finnas andra situationer, som sannolikt innebär en hög risk, då en konsekvens-bedömning ska göras.

Om behandlingen innebär att den personuppgiftsansvarige:

- utvärderar eller poängsätter människor,

- behandlar personuppgifter i syfte att fatta automatiska beslut som har rättsliga följder eller liknande betydande följder för den registrerade,
- systematiskt övervakar människor, till exempel genom kameraövervakning av en allmän plats eller genom att samla in personuppgifter från internetanvändning i offentliga miljöer,
- behandlar känsliga personuppgifter eller uppgifter som är mycket personliga, till lagring av patientjournaler,
- behandlar personuppgifter i stor omfattning,
- kombinerar personuppgifter från två eller flera behandlingar på ett sätt som den registrerade inte förväntar sig, t.ex. när man samkör register,
- behandlar personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara,
- använder ny teknik eller nya organisatoriska lösningar,
- behandlar personuppgifter på ett sätt som hindrar de registrerade från att få tillgång till en tjänst eller ingå ett avtal.

Att utföra en konsekvensbedömning är dock obligatoriskt endast om behandlingen sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. En behandling kan uppfylla två eller flera av ovanstående kriterier men ändå bedömas sannolikt inte leda till en hög risk. I sådana situationer bör den personuppgiftsansvarige motivera och dokumentera anledningarna till att en konsekvensbedömning inte utförs och inkludera dataskyddsombudets synpunkter.

En konsekvensbedömning ska innehålla minst:

- en systematisk beskrivning av den planerade behandlingen och behandlingens syfte.
- en bedömning av om behandlingen är nödvändig och proportionerlig i förhållande till syftet med den.
- en bedömning av riskerna för de registrerades rättigheter och friheter.
- de åtgärder som planeras för att hantera riskerna och för att visa att dataskyddsförordningen efterlevs.

Vidare ska den personuppgiftsansvarige vid utförandet av en konsekvensbedömning:

- rådgöra med dataskyddsombudet Sydarkivera, och
- inhämta synpunkter från de registrerade eller deras företrädare, om det är lämpligt.

4.3 Förhandssamråd

Om risken med en behandling bedöms hög, och fortsatt bedöms hög även efter att planerade åtgärder för att minska riskerna vidtagits ska förhandssamråd med Datainspektionen ske. Vid begäran om samråd ska Datainspektionens blankett, som finns tillgänglig på dess hemsida, användas. Innan förhandssamråd begärs ska riskanalys och konsekvensbedömning gjorts och dokumenterats. Dokumentationen ska också innehålla en redogörelse av vilka risker som kvarstår och varför de inte kunnat åtgärdas.

5. Personuppgiftsbiträde och personuppgiftsbiträdesavtal

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges organisation. En biträdessituation föreligger så snart en aktör behandlar personuppgifter för personuppgiftsansvarig nämnds räkning. Om biträdet behandlar uppgifterna självständigt och själv bestämmer ändamålen med behandlingen föreligger däremot inte en biträdessituation. Om personuppgiftsansvarig nämnd tillsammans med en annan aktör gemensamt bestämmer ändamålen med behandlingen föreligger inte heller en biträdessituation utan ett gemensamt personuppgiftsansvar.

För att agera personuppgiftsbiträde åt Karlshamns kommun ska biträdet kunna lämna tillräckliga garantier för att denne vidtar lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i gällande lagstiftning och säkerställer att den registrerades rättigheter skyddas. Ett personuppgiftsbiträde och dess personal får enbart behandla personuppgifter enligt instruktion från den Karlshamns kommun. Biträdet får inte anlita ett annat biträde utan att i förhand få ett skriftligt tillstånd av personuppgiftsansvarig nämnd.

När en biträdessituation föreligger ska ett personuppgiftsbiträdesavtal upprättas mellan personuppgiftsansvarig nämnd och biträdet.

Personuppgiftsbiträdets behandling av personuppgifter ska regleras i ett personuppgiftsbiträdesavtal mellan personuppgiftsbiträdet och personuppgiftsansvarig nämnd. Vid upphandling av tjänster, system och liknande som innebär att en biträdessituation uppkommer mellan kommunen och leverantören ska kommunens mall för biträdesavtal användas. Om möjligt ska även i andra situationer kommunens mall för biträdesavtal användas. Om biträdet vill använda ett eget avtal ska avtalet granskas så att det uppfyller alla punkter i kommunens checklista för biträdesavtal. Innan leverantörens eget avtal skrivs på ska det skickas till kommunjurist för granskning av biträdesavtalsgruppen.

5.1 Gemensamt personuppgiftsansvar

Om två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen är de gemensamt personuppgiftsansvariga. Gemensamt personuppgiftsansvariga ska fastställa sitt respektive ansvar genom en skriftlig överenskommelse. Överenskommelsen ska innehålla respektive personuppgiftsansvarigs åtaganden för att fullgöra skyldigheterna enligt dataskyddsförordningen, särskilt avseende utövandet av den registrerades rättigheter och skyldigheten att tillhandahålla den registrerade information om behandlingen. Det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade.

Observera att Kommunstyrelsen är personuppgiftsansvarig för de behandlingar som är gemensamma för hela kommunen, d.v.s. exempelvis kommunövergripande system såsom diarieföringssystem.

6. Informationsskyldighet

De registrerade ska få information om att deras personuppgifter behandlas. Artikel 13 och 14 i dataskyddsförordningen ställer långtgående krav på vilken information de registrerade har rätt att få. För att säkerställa att de registrerade får all den information de har rätt till ska kommunens mall för information användas. Den nås via intranätet.

Om personuppgifterna samlas in *från den registrerade själv* behöver den registrerade inte informeras om denne redan har informationen.

Om personuppgifterna samlas in *på något annat sätt än från den registrerade* behöver den registrerade inte informeras om denne redan har fått informationen, om det är omöjligt eller skulle innebära en oproportionerligt stor ansträngning att informera, om registreringen eller utlämnandet av uppgifterna föreskrivs genom lag eller när personuppgifterna omfattas av sekretess enligt lag.

7. Registerförteckning

Varje nämnd ska enligt artikel 30 i dataskyddsförordningen föra ett register över sina behandlingar av personuppgifter. Register ska upprättas skriftligen, vara tillgängliga i elektronisk format och hållas uppdaterade. Detta görs i kommunens system för registerförteckningar (Draftit). Inlogg till systemet lämnas av kommunjurist. Av registret ska minst framgå:

- Namn och kontaktuppgifter för den personuppgiftsansvarige, den personuppgiftsansvariges företrädare samt dataskyddsombudet.
- Ändamålen med behandlingen.
- En beskrivning av kategorierna av registrerade och kategorierna av personuppgifter.
- De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut.
- I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation.
- Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.
- Om möjligt, en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder.

8. Behandling av personuppgifter

Innan behandling av personuppgifter påbörjas krävs följande:

1. Identifiera och dokumentera vilka personuppgifter som kommer att behandlas
2. Dokumentera ändamål och syfte med behandlingen samt hur länge behandlingen beräknas pågå
3. Fastställ laglig grund
4. Inhämta samtycke vid behov
5. Säkerställ att det finns grund för att behandla känsliga personuppgifter om aktuellt
6. Säkerställ att det finns grund för att behandla personnummer om aktuellt
7. Säkerställ att behandlingen sker i enlighet med de grundläggande principerna i dataskyddsförordningen och dataskyddspolicyn samt dessa riktlinjer
8. Rådgör med dataskyddsombudet vid behov
9. Klassificera personuppgifterna utifrån informationsklassningsnivå och genomför en riskanalys av den planerade behandlingen. Dataskyddsombudet ska involveras i riskbedömningen. Vid behov ska en fullständig konsekvensbedömning göras.
10. Samråd med Datainspektionen om konsekvensbedömningen visar att det finns en hög risk med behandlingen som inte kan åtgärdas
11. Se till att det finns tillräckliga tekniska och organisatoriska säkerhetsåtgärder utifrån genomförd informationsklassning och resultatet från riskanalysen
12. Informera den registrerade om behandlingen om det finns ett sådant krav
13. Upprätta personuppgiftsbiträdesavtal vid behov
14. Anteckna ny behandling i nämndens registerförteckning

Noggrann dokumentation av ovanstående punkter ska föras för att visa att kraven i dataskyddsförordningen följs.

9. Personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks.

Exempel på personuppgiftsincidenter är när uppgifter om en eller flera registrerade personer har:

- blivit förstörda
- gått förlorade på annat sätt, eller
- kommit i orätta händer.

Riskerna det medför kan vara till exempel:

- diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning
- finansiell förlust, eller
- brott mot sekretess eller tystnadsplikt.

Personuppgiftsincidenter ska anmälas till Datainspektionen inom 72 timmar efter att de upptäckts. Datainspektionens blankett, som finns på deras hemsida, ska användas. En incident behöver dock inte anmälas om det är osannolikt att den innebär en risk för de registrerade. Då räcker det att motivera beslutet att inte anmäla och noga dokumentera incidenten. Dokumentationen ska omfatta omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits.

Om en incident leder till en hög risk för de registrerade, ska de informeras om incidenten. Risken måste bedömas både utifrån allvarligheten i den potentiella eller faktiska påverkan på personer som ett resultat av en personuppgiftsincident kan ha och sannolikheten för att detta inträffar. Om personuppgiftsincidenten är allvarlig är risken högre. Om sannolikheten för konsekvenser är stor är risken också högre.

När de registrerade ska informeras ska informationen minst innehålla:

- En klar och tydlig beskrivning av orsaken till personuppgiftsincidenten,
- Namn och kontaktuppgifter till dataskyddsombudet eller till en annan kontakt som är insatt i frågan och kan svara på frågor,
- En beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten,
- En beskrivning av de åtgärder som vidtagits, eller kommer att vidtas, för att hantera personuppgiftsincidenten, samt
- En beskrivning av vad ni har gjort för att mildra eventuella negativa effekter.

Beslut att anmäla en personuppgiftsincident samt upprätta anmälan och dokumentation fattas av behörig delegat i enlighet med för respektive nämnd gällande delegationsordning.

Kommunledningsförvaltningen
KARLSHAMNS KOMMUN
Rådhuset, Rådhusgatan 10
374 81 Karlshamn
Telefon: 0454-810 00
karlshamn.se