OSBY KOMMUN

# Personuppgiftsbehandling Dataskydd

Riktlinjer

| | | | |
|---|---|---|---|
| Beslutad av: | Helena Ståhl | Beslutsdatum: | 2019-05-23 |
| Framtagen av: | Lina Bennäs, Informationssäkerhetssamordnare | Dokumentansvarig: | Förvaltningschef |
| Uppdaterad: | | Diarienummer: | HVN/2019:152 |
| | | Giltighetstid | Tillsvidare |

# Innehåll

# 1 Inledning

## 1.1 Bakgrund

Från och med den 25 maj 2018 gäller Dataskyddsförordningens (EU) 2016/679 bestämmelser vid all hantering av personuppgifter i kommunal verksamhet. Dataskyddsförordningen ersätter personuppgiftslagen, PuL (1998:204) och kompletteras av Dataskyddslagen, Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

## 1.2 Syfte

Denna riktlinje ska klargöra hur personuppgifter får behandlas i Osby kommuns verksamheter.

Syftet med dataskyddsförordningen är att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.

## 1.3 Målgrupp

Anställda och förtroendevalda i Osby kommun. Anställda och förtroendevalda i av kommunen helägda aktiebolag i tillämpliga delar.

# 2 Personuppgifter

## 2.1 Personuppgift

Personuppgifter är all information som direkt eller indirekt kan identifiera en levande fysisk person.

## 2.2 Behandling av personuppgift

Alla åtgärder som vidtas i fråga om personuppgifter är en behandling.

# 3 Laglig behandling av personuppgifter

## 3.1 Hantering av personuppgifter

Personuppgifter ska hanteras i enlighet med Dataskyddsförordningens bestämmelser. Dataskyddsförordningen och dataskyddslagen ska inte tillämpas i den utsträckning det strider mot annan lagstiftning.

Varje personuppgiftsbehandling ska ske med hänsyn till den enskildas personliga integritet. Vid varje behandling ska ett sådant förhållningssätt iakttas att risken för den registrerades rättigheter och friheter minimeras.

## 3.2 Rättslig grund

Personuppgifter får inte behandlas utan en rättslig grund.

Minst en av följande lagliga grunder måste fastställas innan personuppgiftsbehandling får ske:

- Behandlingen är nödvändig för att fullgöra ett *avtal.*
- Behandlingen är nödvändig för att fullgöra en *rättslig förpliktelse.*
- 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 personuppgiftsansvarigas *myndighetsutövning*.
- Behandlingen grundar sig på ett aktivt, skriftligt och specifikt *samtycke* där förhållandet mellan den registrerade och kommunen är jämställt. Om den registrerade väljer att inte samtycka till behandling får det inte medföra negativa konsekvenser för den registrerade. Samtycket kan när som helst återkallas. Återkallandet påverkar inte behandlingen innan samtycket återkallades.

## 3.3 Känsliga personuppgifter

Behandling av känsliga personuppgifter är som huvudregel förbjuden.

Känsliga personuppgifter är uppgifter om

- Ras eller etnicitet
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i fackförening
- Genetiska eller biometriska uppgifter som identifierar en individ
- Hälsa, sexualliv eller sexuell läggning

Känsliga personuppgifter får behandlas om den registrerade har lämnat sitt uttryckliga och skriftliga samtycke. Med samtycke jämställs att den registrerade själv på ett tydligt sätt offentliggjort uppgifterna.

Behandling av känsliga personuppgifter utan samtycke kräver lagstöd.

Känsliga personuppgifter får även behandlas utan samtycke när

- Den personuppgiftsansvariga utövar sina skyldigheter inom arbetsrätten
- Den registrerades vitala intressen ska kunna skyddas
- Inom områdena social trygghet eller socialt skydd
- När det är nödvändigt av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin
- Vid bedömning av en arbetstagares arbetskapacitet
- När rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras
- För medicinska diagnoser m.m.

Skyddsåtgärder ska vidtas för att skydda den registrerades grundläggande rättigheter.

## 3.4 Särskilt skyddsvärda personuppgifter

Personnummer eller samordningsnummer får utan samtycke endast behandlas när det är klart motiverat med hänsyn till ändamålet med behandlingen, vid vikten av en säker identifiering eller vid något annat beaktansvärt skäl.

Barns personuppgifter är extra skyddsvärda då barn kan ha svårare att förutse riskerna med att lämna ifrån sig sina uppgifter samt förstå sina rättigheter.

### 3.5 Grundläggande principer

Vid behandling av personuppgifter ska följande grundläggande principer tillämpas

- *Laglighet, korrekthet och öppenhet*
  Personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt gentemot den registrerade. Det måste finnas en rättslig grund för behandlingen och det ska tydligt framgå för den registrerade hur hens personuppgifter samlas in och behandlas.
- *Ändamålsbegränsnin*g
  Innan behandling påbörjas ska ett särskilt och uttryckligt angivet samt berättigat ändamål med behandlingen vara fastställt. Det är inte tillåtet att hantera personuppgifter som inte ryms inom det ursprungliga ändamålet.
- *Uppgiftsminimering*
  Endast de personuppgifter som är adekvata och relevanta för ändamålet får samlas in. Det är inte tillåtet att samla in uppgifter för obestämda framtida behov.
- *Korrekthet*
  Insamlade personuppgifter ska vara korrekta och uppdaterade. Alla rimliga åtgärder ska vidtas för att säkerställa att felaktiga personuppgifter rättas eller raderas utan dröjsmål.
- *Lagringsminimering*
  Insamlade personuppgifter får endast bevaras så länge det är nödvändigt för ändamålet. Efter avslutat ändamål ska uppgifterna raderas, avidentifieras eller arkiveras enligt gällande informationshanteringsplan.

  Insamlade uppgifter får behandlas och lagras under längre tid för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål om det finns lämpliga skyddsåtgärder för den registrerades rättigheter.
- *Integritet och konfidentialitet*
  Personuppgifter ska skyddas mot obehörig eller otillåten behandling, mot förlust, förstöring eller mot skada genom olyckshändelse.
- *Ansvarsskyldighet*
  Personuppgiftsansvarig ansvarar för att all personuppgiftsbehandling som sker under deras ansvar sker enligt dataskyddsförordningens bestämmelser. Personuppgiftsansvarig ska kunna visa *att* och *hur* bestämmelserna i förordningen efterlevs.

  Exempel på åtgärder som ska vidtas för att visa att förordningen följs

  - Tydlig information till den registrerade om hur hens personuppgifter behandlas samt information om hens rättigheter gentemot den personuppgiftsansvariga
  - Upprättande av registerförteckning
  - Upprättande av interna styrdokument
  - Utbildning av personal
  - Dokumenterade konsekvensbedömningar

- Dokumenterade ställningstaganden vid alla personuppgiftsbehandlingar.

# 4 Personuppgiftsansvarig

Den personuppgiftsansvariga är en fysisk eller juridisk person eller myndighet som bestämmer ändamål och medel för behandlingen av personuppgifter. Den personuppgiftsansvariga har det ytterst juridiska ansvaret för att lagstiftningen efterlevs. Den faktiska behandlingen av personuppgifter kan överlåtas men aldrig det yttersta ansvaret.

I Osby kommun är Kommunstyrelsen, Barn- och utbildningsnämnden, Hälsa och välfärdsnämnden, Miljö- och byggnämnden samt Samhällsbyggnadsnämnden personuppgiftsansvariga för respektive verksamhet. Kommunägda bolag är enskilt personuppgiftsansvariga.

Ansvaret innebär bland annat att

- Fastställa rättslig grund vid all personuppgiftsbehandling
- Utse dataskyddsombud
- Säkerställa att tekniska och organisatoriska förutsättningar finns så att alla personuppgifter behandlas med erforderlig säkerhet
- Kunna visa att kraven i lagstiftningen uppfylls
- Föra register över de personuppgiftsbehandlingar som sker inom verksamheten.

Respektive personuppgiftsansvarig i Osby kommun ska utse lokala GDPR-ombud som arbetar löpande med dataskyddsförordningen.

# 5 Personuppgiftsbiträde

Ett personuppgiftsbiträde är en fysisk eller en juridisk person som externt hanterar personuppgifter på uppdrag av den personuppgiftsansvariga.

## 5.1 Personuppgiftsbiträdesavtal

Ett personuppgiftsbiträdesavtal reglerar hur biträdet får behandla personuppgifter för den personuppgiftsansvarigas räkning. Avtalet säkerställer att personuppgiftsbiträdet upprätthåller lämplig teknisk och organisatorisk säkerhet i enlighet med gällande rätt.

Avtal ska alltid upprättas innan personuppgiftsbehandling påbörjas.

Personuppgiftsbiträdesavtal ska inte tecknas internt inom kommunen.

I reglementet för Osby kommuns nämnder anges vilken nämnd som är personuppgiftsansvarig för respektive kommunövergripande verksamhetssystem.

Vid gemensamt personuppgiftsansvar mellan två eller fler av kommunens nämnder ska ansvarsfördelningen för behandlingarna dokumenteras.

# 6 Registerförteckning

Varje personuppgiftsansvarig ska föra ett register över de personuppgiftsbehandlingar som utförs under deras ansvar. Registret är en

förteckning över alla system, dokument och övriga register där personuppgifter förekommer. Registret är ett levande dokument och ska vid behov revideras.

# 7 Dataskyddsombud

Dataskyddsombudets uppgift är att informera och ge råd till personuppgiftsansvarig om skyldigheterna enligt dataskyddsförordningen.

Dataskyddsombudet ska även övervaka efterlevnad av förordningen samt ge råd vid konsekvensbedömningar. Den personuppgiftsansvariga ska säkerställa att dataskyddsombudet involveras i alla frågor som rör skyddet av personuppgifter.

# 8 Den registrerades rättigheter

## 8.1 Rättigheter

Den personuppgiftsansvariga ska vidta lämpliga åtgärder för att tillhandahålla den registrerade klar och tydlig information gällande de personuppgiftsbehandlingar som utförs om hen samt klar och tydlig information om den registrerades rättigheter.

Vid begäran om att utöva sina rättigheter ska myndigheten svara den registrerade snarast, dock senast inom en (1) månad efter mottagen begäran.

När den registrerade använder sina rättigheter ska besvärshänvisning bifogas den personuppgiftsansvarigas beslut.

### 8.1.1 Rätt till information och tillgång

Den registrerade har rätt att få information om att hens personuppgifter behandlas av Osby kommun. Information ska lämnas i samband med mottagandet av uppgifterna eller vid första registreringstillfället. Information får inte lämnas senare än en månad efter mottagande av uppgifterna.

Informationen ska vara tydlig och omfatta

- Ändamålet med behandlingen
- Vilka kategorier av personuppgifter som behandlas
- Den rättsliga grund på vilken uppgifterna behandlas
- Mottagare av uppgifterna
- Hur länge uppgifterna ska sparas
- Den registrerades rättigheter
- Rätten att ta tillbaka ett eventuellt samtycke
- Rätten att lämna klagomål till Datainspektionen
- Information om ifall att uppgifterna ska överföras till ett tredje land
- Källan som uppgifterna har hämtats från
- Information om ifall att automatiserat beslutsfattande förekommer
- Kontaktuppgifter till den personuppgiftsansvariga samt dess dataskyddsombud.

Information behöver inte lämnas till den registrerade om det finns andra bestämmelser som gäller framför dataskyddsförordningen, exempelvis vid sekretessklassade uppgifter. Information behöver heller inte lämnas om den

registrerade redan har fått informationen eller om det är omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

#### 8.1.2 Rätt till rättelse och radering

Den registrerade har rätt att vända sig till den personuppgiftsansvariga med begäran om att få felaktiga personuppgifter rättade.

Kommunala myndigheter får inte gallra (radera) eller rätta i allmänna handlingar utan att det anges i lag eller i myndighetens fastställda informationshanteringsplan.

Uppenbara skrivfel i myndighetsbeslut får rättas enligt 36§ Förvaltningslagen (2017:900).

Personuppgifter kan raderas om behandlingen grundar sig på den registrerades samtycke och hen återkallar samtycket.

Om personuppgiftsansvarig har lämnat ut uppgifterna till en tredje part ska denna meddelas om rättelsen.

#### 8.1.3 Rätt till begränsning av behandling

Den registrerade har rätt att begära att behandlingen av hens personuppgifter begränsas och endast får användas för vissa avgränsade syften.

Rätt till begränsning gäller bland annat när den registrerade anser att uppgifterna är felaktiga och har begärt rättelse. I sådana fall kan den registrerade begära att behandlingen av uppgifter begränsas under tiden uppgifternas korrekthet utreds. När begränsningen upphör ska den registrerade informeras om detta.

#### 8.1.4 Rätt till dataportabilitet

Den registrerade har rätt till dataportabilitet vilket innebär att personuppgifter flyttas, kopieras eller överförs från en IT-miljö till en annan. Denna rättighet är endast tillämplig då den registrerade själv har lämnat uppgifterna till myndigheten samt då behandlingen grundar sig på samtycke eller avtal.

#### 8.1.5 Rätt att göra invändningar

Den registrerade har rätt att invända mot personuppgiftsbehandling när personuppgifter behandlas för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning.

Om den registrerade invänder mot behandling får den personuppgifts-ansvariga endast fortsätta med behandlingen om det finns skäl som väger tyngre än den registrerades intressen, rättigheter och friheter eller om behandlingen sker för fastställande, utövande eller försvar av rättsliga anspråk.

Särskilda regler gäller för personuppgifter som behandlas för vetenskapliga och historiska forskningsändamål eller statistiska ändamål.

### 8.2 Begäran om registerutdrag

Den registrerade har rätt att få en skriftlig, samlad förteckning över de personuppgifter som myndigheten behandlar om hen.

Registerutdraget ska tillhandahållas den registrerade kostnadsfritt och vara formulerat med ett enkelt och tydligt språk.

Uppgifterna får inte lämnas ut om det strider mot annan lagstiftning eller registerförfattning.

Registerutdrag ska tillhandahållas den registrerade inom en månad efter mottagen begäran. Särskilda skäl måste föreligga om registerutdraget försenas.

## 9 Personuppgiftsincident

En personuppgiftsincident är en händelse som har påverkat sekretessen, integriteten eller tillgängligheten till de personuppgifter som behandlas av personuppgiftsansvarig. Incidenten kan innebära risk för människors rättigheter och friheter, så som risk för diskriminering, identitetstöld, bedrägeri, skadlig ryktesspridning, finansiell förlust eller brott mot sekretess och tystnadsplikt.

Incidenter ska vid risk för den registrerades friheter och rättigheter anmälas till Datainspektionen inom 72 timmar efter upptäckt. Vid stor risk för den registrerades rättigheter och friheter ska den registrerade snarast få information om det inträffade.

## 10 Säkerhet

Behandling av personuppgifter får endast ske om lämplig teknisk och organisatorisk säkerhet vidtagits för behandlingen.

Säkerhet ska utgöras av inbyggt dataskydd och dataskydd som standard. Integritets- och dataskyddsprinciperna ska beaktas från den initiala planeringen av all personuppgiftsbehandling. Personuppgifter ska som standard behandlas med högsta integritetsskydd.

## 11 Införskaffande av appar eller IT-system

Vid införskaffande av nya appar eller IT-system ska personuppgiftsansvarig ta hänsyn till skyddet av personuppgifter samt säkerställa att systemet har erforderliga sök- och gallringsmöjligheter.

## 12 Konsekvensbedömning

Om en personuppgiftsbehandling sannolikt leder till risk för den registrerades rättigheter och friheter ska en konsekvensbedömning utföras. Bedömningen ska analysera riskerna med behandlingen samt föreslå lämpliga säkerhetsåtgärder. Bedömningen ska noggrant dokumenteras. Dataskyddsombudet ska involveras vid alla konsekvensbedömningar.

Syftet med konsekvensbedömningen är bland annat att

- Förebygga risker innan de uppkommer
- Bedöma om uppgifterna som samlas in är nödvändiga för ändamålet
- Bedöma om den personuppgiftsansvariga har vidtagit tillräckliga åtgärder för att skydda den registrerades rättigheter och friheter.

I fall då vidtagna åtgärder ändå leder till en hög risk för den registrerades rättigheter ska samråd ske med Datainspektionen innan behandling får påbörjas.