Åtvidabergs kommun

Riktlinje för hantering av personuppgifter Åtvidabergs kommun

ÅKF: 2019:09
Dnr: ATVKS 2018-00473 003
Antagen: Kommunfullmäktige § 77, 2019-05-29
Reviderad:-
Dokumentansvarig förvaltning: Kommunledningsförvaltningen, kanslienheten
Dokumentet gäller för: Åtvidabergs kommun
Dokumentet gäller till och med: 2022-12-31

Innehållsförteckning

Inledning och syfte

Åtvidabergs kommuns riktlinjer för hantering av personuppgifter är ett komplement till kommunfullmäktiges policy för hantering av personuppgifter. Riktlinjerna gäller för kommunens samtliga nämnder, bolag och stiftelser.

Policyn och riktlinjernas syfte är dels att säkerställa att Åtvidabergs kommun hanterar personuppgifter på ett lagenligt sätt men också att visa för allmänhet och anställda att de kan känna sig trygga med att deras personuppgifter hanteras på respektfullt sätt och att inga personuppgifter hanteras i onödan eller riskerar att hamna i orätta händer.

Nämndernas ansvar

Varje nämnd, bolag och stiftelse är personuppgiftsansvarig för behandlingen av personuppgifter inom sitt verksamhetsområde. Nämnderna ansvarar för att kraven som ställs på personuppgiftsansvariga i dataskyddsförordningen uppfylls. Ansvaret innebär en yttersta skyldighet att tillse att gällande lagstiftning efterlevs 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 den kunskap som krävs för att fullgöra sitt uppdrag.
- Säkerställa att det finns tekniska och organisatoriska förutsättningar att behandla personuppgifter med nödvändig säkerhet.
- Kunna visa att krav i lagstiftning är uppfyllda genom noggrann dokumentation samt verifierande tester.
- Föra register över behandlingar av personuppgifter i Åtvidabergs kommuns gemensamma registerverktyg.

Särskilt om kommunstyrelsen

Kommunstyrelsen är personuppgiftsansvarig för samtliga behandlingar som rör kommunövergripande system till exempel hemsida, HR-relaterad verksamhet, ekonomi, e-post, telefoni med mera.

Kommunstyrelsen har genom sin uppsiktsplikt över nämnderna ett särskilt ansvar för att kommunens behandling av personuppgifter. Kommunstyrelsen ska inom ramen för uppsiktsplikten vid behov ge nämnderna råd, anvisningar och förslag på åtgärder. Om dessa inte följs av nämnderna sak kommunstyrelsen initiera ärende i fullmäktige för att utfärda bidande direktiv till nämnderna.

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:

- 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 att utföra uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

All behandling av personuppgifter ska dokumenteras i enlighet med EU´s dataskyddsförordning. Ansvarsskyldigheten är en grundläggande princip vilken ställer krav på att den personuppgiftsansvarige ska kunna att krav och principer följs och på vilket sätt detta görs. Varvid den personuppgiftsansvarige ska förfara med dokumenterad information vad gäller fastställt, styrande och stödjande dokumentation (innefattar fastställda metodstöd). Innan behandling av personuppgifter påbörjas krävs följande:

1. Dokumentation av 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. Rådgör med dataskyddsombudet vid konsekvensbedömningar av behandling av personuppgifter som kan leda till en hög risk för de registrerade
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. Anteckna ny behandling av personuppgifter i kommunens registerverktyg.

Dataskyddsorganisation - verksamhet

Kommunchef

Kommunchefen ansvarar för att den kommunala verksamheten har en fungerade dataskyddsorganisation.

Förvaltningarna

Varje förvaltning ska kunna visa att den innehar rätt resurser och relevant kompetens inom området för att kunna följa EU´s dataskyddsförordning, de nationella dataskyddsbestämmelserna samt dessa riktlinjer.

Lokala dataskyddsamordnare

Varje förvaltning och de kommunala bolagen ska utse minst en lokal dataskyddsamordnare med ansvar för att arbeta löpande med frågor relaterade till dataskyddsförordningen. Den eller de lokala dataskyddsamordnarna ska ha ett uttalat och dokumenterat uppdrag och avsatt arbetstidsmått för att arbeta med dataskyddsfrågor.

Finns flera lokala dataskyddsamordnare inom förvaltningen ska en utses som förvaltningens kontaktperson för dataskyddsfrågor med uppgift att fungera som en länk mellan förvaltningens verksamheter, dataskyddsombudet och kommunens centrala dataskyddsamordnare för dataskyddsfrågor.

Central dataskyddsamordnare

På kommunledningsförvaltningen ska det finnas en central dataskyddsamordnare med ansvar för att samordna kommunens övriga lokala dataskyddsamordnare, hålla kontakt med dataskyddsombudet och i övrigt vara förvaltningarna behjälplig med råd och stöd i frågor rörande dataskyddsdirektivets genomförande. Den centrala dataskyddsamordnaren ska ha ett uttalat och dokumenterat uppdrag och avsatt arbetstidsmått för att arbeta med dataskyddsfrågor.

Kommunledningsförvaltningens dataskyddsamordnare ansvarar vidare för

- Hålla den information om kommunens hantering av personuppgifter som ska finnas på kommunens hemsida uppdaterad.
- Hålla kontaktuppgifter gällande dataskyddsombud uppdaterade på kommunens hemsida samt meddela dessa till dataskyddsmyndigheten.
- Samla in och sammanställa nämndernas, förvaltningarnas och kommunalförbundet ITSAM årliga rapportering.
- Identifiera förekomsten av generella svårigheter och problem i förvaltningarna och i samråd med dataskyddsombudet ta fram förslag till lämpliga åtgärder
- Bistå förvaltningarna med råd och stöd i frågor relaterade till efterlevnaden av EU´s dataskyddsförordning och nationell dataskyddslagstiftning.
- Administrera och fortlöpande uppdatera ansvarsfördelningen samt särskilda säkerhetsinstruktioner mellan Åtvidabergs kommuns nämnder (inkl. kommunstyrelsen) avseende de personuppgifter som behandlas för en annan nämnds vägnar, alternativt då ett gemensamt personuppgiftsansvar föreligger två eller flera nämnder emellan.

Kommunens lokala dataskyddssamordnare och dataskyddsombudet ska sammanträda gemensamt minst en gång årligen. Sammanträdena ska sammankallas och ledas av kommunalförbundet ITSAMs dataskyddsombud.

Informationssäkerhetsansvarig/samordnare

På kommunledningsförvaltningen ska det finnas en funktion för samordning av informationssäkerhet. Informationssäkerhetssamordnaren har i uppdrag att leda och samordna kommunens informationssäkerhetsarbete.

Behandlings- och registeransvariga

För varje behandling och personuppgiftsregister ska det finnas en ansvarig tjänsteman med uppgift att för personuppgiftsansvarig styrelse, nämnd, bolag eller stiftelse säkerställa att behandlingen sker i enligt med gällande föreskrifter.

Ansvarig är normalt den tjänsteman/chef som har det operativa ansvaret för personuppgiftsbehandlingen.

Återrapportering av personuppgiftsbehandling

Nämnderna och förvaltningarna underlydande kommunstyrelsen och kommunalförbundet ITSAM ska årligen skriftligen rapportera sitt arbete enligt dessa riktlinjer, dataskyddsförordningen och övriga dataskyddsbestämmelser till kommunstyrelsen.

Närmare instruktioner kring innehållet i återrapporteringen tas fram av kommunens centrala dataskyddsamordnare i samråd med dataskyddsombudet.

Dataskyddsombud

Varje nämnd ska utnämna ett dataskyddsombud som ska rapportera direkt till förvaltningsledningen. Åtvidabergs kommun samverkar med kommunalförbundet ITSAM gällande dataskyddsombud. Nämnderna ska därmed utse denna som dataskyddsombud.

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 dataskyddsmyndigheten.
- Vara kontaktpunkt för tillsynsmyndigheten i alla frågor som rör behandling av personuppgifter.
- Företräda de 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.
- Upprätthålla ombudets 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.
- Dataskyddsombudet ska årligen redovisa för de personuppgiftsansvariga nämnderna det arbete som verksamheten gör gällande efterlevnaden av dataskyddsdirektivet, nationell dataskyddslagstiftning och lokala styrdokument. Av den årliga redovisningen ska det minst framgå:
    - Vilka interna och externa utbildningsåtgärder som förvaltningen genomfört på området
    - Vid vilka ledningsgruppsmöten som dataskyddsombudet har beretts tillfälle närvara vid för att avlägga rapport över förvaltningens hantering av personuppgifter
    - Tekniska brister som åtgärdats under året
    - Tekniska brister som bör åtgärdas
    - Eventuella personuppgiftsincidenter
    - Övriga iakttagelser

Dataskyddsombudet ska när denna anser det nödvändigt ges tillträde till förvaltningarnas ledningsgrupper. Den personuppgiftsansvarige bör av detta skäl meddela personuppgiftsombuden och sammankomster som avhandlar data och integritetsskydd eller alternativt informationssäkerhetsaspekter.

Förvaltningsledningarna ska säkerställa att dataskyddsombudet involveras och rådfrågas på ett så tidigt stadium som möjligt när behandling av personuppgifter kan komma ifråga.

Tjänster, produkter och applikationer som medför behandling av personuppgifter

För varje tjänst, produkt och applikation som används eller som det finns planer på att använda ska särskilt beaktas om avtalsförhållandet eller användandet av produkten eller applikationen kan komma att medföra behandling av personuppgifter. För det fall personuppgifter kommer att behandlas ska, med hänsyn till den tekniska utvecklingen, säkerställas att det finns tekniska förutsättningar för såväl förvaltningen som för dess personuppgiftsbiträde att kunna fullgöra sina skyldigheter avseende dataskydd.

Särskilt vid inköp och upphandling

Vid inköp och upphandlingar (av produkter och tjänster) ska särskilt utredas om användandet av det som inköpet avser eller annars som en följd av avtalsrelationen kan komma att leda till behandling av personuppgifter. Förvaltningarna ska ha en rutin för under vilka förutsättningar dataskyddsombudet ska engageras vid inköp och upphandlingar och när under inköpsprocessen som denne bör kontaktas.

Vid inköp och upphandlingar av produkter och tjänster som kan komma att leda till behandling av personuppgifter ska krav ställas på att all utrustning lever upp till kraven i dataskyddsförordningen och annan lagstiftning inom dataskyddsområdet.

Vid utredning av vilka tekniska säkerhetskrav som bör ställas ska, vid behov, samråd ske med Kommunalförbundet ITSAM.

Konsekvensbedömning avseende dataskydd

En konsekvensbedömning ska enligt dataskyddsförordningen göras om en viss personuppgiftsbehandling "sannolikt leder till en hög risk för fysiska personers rättigheter och friheter". Risken ska i första hand bedömas utifrån dataskydd och integritet, men även utifrån andra grundläggande rättigheter som yttrandefrihet, tankefrihet, fri rörlighet, förbud mot diskriminering, rätt till frihet, samvete och religion.

Konsekvensbedömningar handlar om att vara förutseende, förebygga risker och därmed skydda människors fri- och rättigheter. Målet är att minimera riskerna vid sådana behandlingar av personuppgifter som innebär en hög risk för enskilda personers fri- och rättigheter samt göra en bedömning om behovet av behandlingen och det intrång den utgör står i proportion till syftet

Men en regelrätt konsekvensbedömning behöver inte alltid göras:

1. Analysera vilka risker behandling av personuppgifter kan innebära och föreslå lämpliga säkerhetsåtgärder. Dokumentera resultatet av analysen, så att ni kan visa att ni följer förordningen.

2. Utifrån riskanalysen beslutar förvaltningen om en konsekvensbedömning behöver genomföras.

Konsekvensbedömning är ett viktigt verktyg eftersom det hjälper oss att:

- uppfylla kraven i dataskyddsförordningen
- hantera risker för att man inte uppfyller dataskyddsförordningen
- visa att kommunen uppfyller dataskyddsförordningen

All personuppgiftsbehandling ska regelbundet och kontinuerligt ses över och omvärderas för att bedöma om det behövs en konsekvensbedömning. Förhållanden kan ändras så att även personuppgiftsbehandlingar som tidigare inte konsekvensbedömts kan behöva genomlysas om förutsättningarna ändrats.

En genomförd konsekvensbedömning kan användas för att bedöma flera personuppgiftsbehandlingar sin liknar varandra vad gäller art, omfattning, innehåll, ändamål och risker.

Incidentrapportering

I dataskyddsförordningen definieras en personuppgiftsincident som "en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats".

Alla organisationer är enligt dataskyddsförordningen skyldiga att ha rutiner för att kunna upptäcka, rapportera och utreda personuppgiftsincidenter.

Varje förvaltning ska kunna upptäcka, hantera och rapportera personuppgiftsincidenter som sker inom den egna verksamheten.

Vad är en personuppgiftsincident?

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:

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

En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har

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

Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. I båda fallen är det personuppgiftsincidenter.

En personuppgiftsincident kan få allvarliga konsekvenser för registrerade personer. De kan råka ut för till exempel ekonomisk skada eller kränkning av sina friheter och rättigheter.

En personuppgiftsincident som inte hanteras på ett lämpligt sätt kan också påverka tilltron till den organisation som behandlar personuppgifter. Bristande hantering av personuppgiftsincidenter kan leda till sanktionsavgifter.

Vad ska rapporteras?

Samtliga incidenter ska rapporteras till dataskyddsombudet.

När det har inträffat en personuppgiftsincident måste förvaltningen först fastställa sannolikheten och allvaret, och den därmed följande risken för människors rättigheter och friheter, d v s vilka konsekvenser personuppgiftsincidenten kan leda till.

- Hur allvarliga kan konsekvenserna bli?
- Hur sannolikt är det att enskilda personer drabbas?

Om personuppgiftsincidenten är allvarlig är risken högre. Om sannolikheten för konsekvenser är stor är risken också högre.

Om det är troligt att personuppgiftsincidenten kommer att medföra en risk för de registrerade måste förvaltningen anmäla detta till Datainspektionen. Men om det är osannolikt att en personuppgiftsincident medför risker behöver förvaltningen inte meddela Datainspektionen.

Incidenter som leder till minst ”betydande skada” enligt skalan nedan ska i Åtvidabergs kommun rapporteras till Datainspektionen inom 72 timmar från det att incidenten inträffade.

Bedömd skada

Vid rapportering av incident ska eventuell skada bedömas enligt följande nivåer:

- Allvarlig skada - ex massiv informationsförlust, verksamhetsförlust, oöverskådliga konsekvenser, samt fara för liv och hälsa
- Betydande skada - ex tillgänglighetsstörningar, brott mot regelverk, rättsliga krav och avtal, samt förlust av skapat förtroende
- Måttlig skada - ex minskad förmåga att genomföra verksamhetens uppgifter, men effektiviteten är påvisbart reducerad
- Försumbar skada

Rapportering inom 72 timmar

Om rapporteringen till dataskyddsmyndigheten görs efter det att 72 timmar förflutit från det att personuppgiftsincidenten upptäcktes ska förseningen motiveras. Rapportering till dataskyddsmyndigheten behöver emellertid inte göras om det är osannolikt att incidenten kan komma att medföra en risk för de registrerades grundläggande fri- och rättigheter.

Registrering

Alla personuppgiftsincidenter ska registreras i kommunens ärendehanteringssystem.

Vem ska anmäla incidenten?

Anmälan görs av den personuppgiftsansvarige, det vill säga den myndighet eller annan organisation som bestämmer ändamål och medel för behandlingen. Men det finns också en skyldighet för den som har anlitats som personuppgiftsbiträde att uppmärksamma den personuppgiftsansvarige på en säkerhetsincident så fort den upptäckts.

I Åtvidabergs kommun anser vi att incidentrapportering är en verkställighets åtgärd som ska hanteras inom respektive förvaltningen. Varje förvaltning ska därför ha en rutin där det framgår hur en personuppgiftsincident ska hanteras internt inom förvaltningen och vem som ska ansvara för att rapporteringen till dataskyddsmyndigheten ska kunna göras inom 72 timmar från upptäckt.

Anmälan till Datainspektionen

Personuppgiftsincidenter anmäls genom att Datainspektionens blankett ”Anmälan om personuppgiftsincident” används. Blanketten återfinns på Datainspektionens hemsida.

Information till registrerade personer

Om personuppgiftsincidenten är allvarlig så ska förvaltningen utan onödigt dröjsmål även informera de registrerade om personuppgiftsincidenten. Detta gäller alltså om det är sannolikt att personuppgiftsincidenten leder till en hög risk för fysiska personers rättigheter och friheter.

Följande punkter är ett minimikrav när information ska ges till registrerade utifrån en inträffad personuppgiftsincident:

- Orsaken till personuppgiftsincidenten klart och tydligt.
- Namn och kontaktuppgifter till dataskyddsombudet,
- De sannolika konsekvenserna av personuppgiftsincidenten.
- Vilka åtgärder förvaltningen gjort och/eller tänker göra, för att hantera personuppgiftsincidenten.
- I förkommande fall: Beskriv vad förvaltningen har gjort för att mildra eventuella negativa effekter.

Information dataskyddsombud

Dataskyddsombud ska alltid informeras om uppstådda personuppgiftsincidenter.

Säkerhet i samband med behandlingen

Varje nämnd ansvarar för att en fullgod säkerhetsnivå upprätthålls vid behandling av personuppgifter. Förvaltningarna ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå utifrån de kriterier som anges i dataskyddsförordningen.

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 säkerhetsåtgärder i enlighet med informationsklassningens åtgärdsplan vidtas.
  - Om möjligt använda åtgärder som pseudonymisering, anonymisering eller kryptering.
  - Säkerställa särskilda personuppgifters konfidentialitet och riktighet genom att bl.a. använda kryptering samt stark autentisering.
  - Använda åtgärder som uppgiftsminimering, lagringsminimering, fritextfältsmimimering 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.

För frågor som gäller tekniska åtgärder gällande IT-verksamhet ansvarar kommunalförbundet ITSAM.

Vid planering av verksamheten ska särskild hänsyn tas till att personuppgifter inte behandlas i högre utsträckning eller under längre tid än vad som är nödvändigt. Anställda som på något sätt kan komma att behandla personuppgifter i sitt arbete ska genomgå utbildning för att säkra att personuppgifter hanteras på ett lagligt och respektfullt sätt.

Kontroll över personuppgiftsbehandlingar

Nämnderna ansvarar för att av de personuppgifter som behandlas inom ramen för dess verksamhet sker på ett lagenligt sätt.

Register över personuppgiftsbehandlingar

Varje nämnd ska löpande föra ett register över vilka personuppgifter som behandlas i den egna verksamheteten i de kommungemensamma registersystemet.

Registret ska föras utifrån instruktioner från kommunledningsförvaltningen, kanslienheten.

Personuppgiftsbiträdesavtal och gemensamt personuppgiftsansvar

Personuppgiftsbiträdesavtal

Varje nämnd ska teckna personuppgiftsbiträdesavtal när denne uppdrar åt ett externt personuppgiftsbiträde att behandla uppgifter. Vem som får underteckna personuppgiftsbiträdesavtalet ska framgå av nämndens delegationsordning.

Förvaltningarna ska föra en förteckning över aktuella personuppgiftsbiträdesavtal och därtill hörande underbiträdesavtal.

Kommunen som personuppgiftsansvarig ska teckna personuppgiftsbiträdesavtal med ITSAM, vilket ska reglera hur ITSAM i sina led får behandla och lagra personuppgifter.

Kommunalförbundet ITSAM ansvarar för att teckna personuppgiftsbiträdesavtal med de leverantörer som förbundet tecknar avtal med. Dessa leverantörer blir därmed underbiträden till ITSAM i förbundets relation till kommunen.

Personuppgiftsbiträdets (biträdet) behandling av personuppgifter ska regleras av personuppgiftsbiträdesavtal mellan biträdet och den personuppgiftsansvarige (ansvarige). I avtalet ska 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 nödvändig 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 avtalets upphörande.

Avtal vid gemensamt personuppgiftsansvar

För de fall där det föreligger ett gemensamt personuppgiftsansvar med en extern part ska nämnden tillse att det tecknas ett avtal där de personuppgiftsansvarigas respektive ansvar för att fullgöra skyldigheterna enligt EU´s dataskyddsförordning och andra nationella dataskyddsbestämmelser fastställs.

Förvaltningarna ska föra en förteckning över aktuella avtal som ger styrning för gemensamt personuppgiftsansvar.

Personuppgiftsbiträdesavtal och gemensamt personuppgiftsansvar mellan stadens nämnder

Kommunledningsförvaltningen, kanslienheten ska administrera en förteckning över ansvarsfördelningen och de särskilda säkerhetsinstruktioner mellan kommunens nämnder (inkl. kommunstyrelsen) avseende de personuppgifter som behandlas för en annan nämnds vägnar, alternativt då ett gemensamt personuppgiftsansvar föreligger två eller flera nämnder emellan.

Förteckningen ska uppdateras löpande men ska som minst godkännas årligen av kommunstyrelsen.

Registrerades rättigheter

Information till de registrerade

Varje förvaltning ska ha rutiner för hur information ska tillhandahållas till de registrerade. Informationsmaterial ska i så stor utsträckning som möjligt tas fram gemensamt.

Tillgång, rättelse, radering och begränsning

Varje förvaltning ska ha rutiner för hantering av begäranden från registrerade om att utöva sina rättigheter att:

- Få tillgång till information om dennes personuppgifter.
- Rätta eller komplettera sina uppgifter.
- Rader sina uppgifter
- Begränsa sina uppgifter
- Utnyttja möjligheten till dataportabilitet om sådan möjlighet finns.

Det ska av respektive nämnds delegationsordning framgå vem som äger rätt att fatta beslut enligt dataskyddsförordningen och tillämplig nationell dataskyddslagstiftning.

Övergripande kommungemensamma rutiner ska i stor utsträckning tas fram.