Beslutsinstans: Kommunfullmäktige
Processägare: Digitaliserings- och utvecklingschef

Senast uppdaterad: 2025-x
Styrdokumentsnummer: DK 2025:x

# Reglemente för dataskydd

*Reglering av personuppgiftsansvar mellan nämnder inklusive Djursholms AB*

## Dokumentets syfte

Reglementet syftar till att reglera personuppgiftsansvar mellan nämnderna och i relation till Djursholms AB.

## Dokumentet gäller för

Reglementet gäller för samtliga nämnder och Djursholms AB i Danderyds kommun.

# Innehåll

# Bakgrund

Varje nämnd är i enlighet med det egna reglementet personuppgiftsansvarig för behandling av personuppgifter inom nämndens verksamhet. Behandlingar där det föreligger ett internt biträdesförhållande, eller ett gemensamt personuppgiftsansvar, ska regleras genom en särskild rättsakt. För varje behandling av personuppgifter krävs att personuppgiftsansvaret för behandlingen regleras, och varje nämnd har en ansvarsskyldighet för att kunna visa att dataskyddsförordningen efterlevs.

Det som fastställs med detta reglemente är styrande för samtliga nämnder och i relation till Djursholms AB.  Nämnderna och Djursholms AB har inte möjlighet att besluta om avvikelser från detta reglemente.

## Personuppgiftsansvar i kommun

I en kommun kan det mellan nämnderna förekomma

- självständigt personuppgiftsansvar (varje nämnd är ensamt ansvarig)
- gemensamt personuppgiftsansvar (två, eller fler nämnder är gemensamt ansvariga för en personuppgiftsbehandling) eller
- biträdesförhållande (en nämnd hanterar personuppgifter för en annan nämnds räkning och utgör då ett biträde till den personuppgiftsansvariga nämnden).

## Ansvarsfördelning vid gemensamt personuppgiftsansvar artikel 26 dataskyddsförordningen

Vid gemensamt personuppgiftsansvar mellan två eller flera nämnder ansvarar varje nämnd för den behandling som sker inom dess egen verksamhet. För vissa specifika situationer har ansvaret fördelats enligt nedanstående.

## Behandlingsregister, artikel 30 dataskyddsförordningen

Varje personuppgiftsansvarig och, i tillämpliga fall, dess företrädare ska föra ett register över behandling som utförts under dess ansvar.

- Gemensamma personuppgiftsbehandlingar ska registreras i kommunens behandlingsregister avsett för gemensamma personuppgiftsbehandlingar. Det ska dokumenteras vilka nämnder personuppgiftsbehandlingen är gemensamma för.

- Kommunstyrelsen ansvarar för att tillhandahålla och förvalta systemverktyget för dataskydd.
- Nämnderna ansvarar för att i dialog med kommunstyrelsen säkerställa att deras gemensamma behandlingar registreras i det gemensamma behandlingsregistret

## Risk- och konsekvensanalys, artikel 35 dataskyddsförordningen

Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker.

- Den nämnd som är systemägare för systemet, där den huvudsakliga behandlingen sker, ansvarar för att samordna genomförandet av risk- och konsekvensbedömning för behandlingen.
- Dokumentation av risk- och konsekvensförteckning ska dokumenteras i anvisat systemstöd.
- Vardera personuppgiftsansvarig nämnd ansvarar för att vidta de tekniska och organisatoriska säkerhetsåtgärder som krävs utifrån dels personuppgiftsbehandlingens art, dels vad konsekvensbedömningen visar.

## Förhandssamråd, artikel 36 dataskyddsförordningen

Den personuppgiftsansvarige ska samråda med tillsynsmyndigheten före behandlingen om en konsekvensbedömning avseende dataskydd enligt artikel 35 visar att behandlingen skulle medföra en hög risk, om inte åtgärder vidtas för att minska risken.

- Den nämnd som är systemägare, där den huvudsakliga behandlingen sker, ansvarar för att samordna handläggning, beslut och begäran om förhandssamråd samt att säkerställa ett genomförande av förhandssamrådet.

## Personuppgiftsincidenter, artikel 4 p 12 och 33 dataskyddsförordningen

En personuppgiftsincident är 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.

Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig i enlighet med artikel 55, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.

- Den nämnd som är systemägare för systemet, där incidenten huvudsakligen skett, ansvarar för att samordna utredning, de beslut som incidenten föranleder och vid behov anmälan till Integritetskyddsmyndigheten.
- Information rörande incidenten ska lämnas till vardera berörd nämnd.
- Vardera personuppgiftsansvarig nämnd ansvarar för att vidta de åtgärder som krävs med anledning av inträffad incident.

## Revision och tillsyn

- Alla gemensamt personuppgiftsansvariga nämnder kan initiera revision och tillsyn gentemot ett personuppgiftsbiträde.
- Den nämnd som tecknat personuppgiftavtalet ansvarar för att genomföra en revision och/eller tillsynen.
- Den nämnd som är systemägare för systemet där den huvudsakliga behandlingen sker, är kontaktpunkt vid tillsyn av Dataskyddsombudet eller Integritetsskyddsmyndigheten.

## Upphandling och implementering av upphandlad tjänst/produkt

Vid upphandling som omfattar gemensamma personuppgiftsbehandlingar:

- ansvarar beställaren för att säkerställa att upphandlingens omfång och behov är utrett av berörda nämnder.
- ansvarar beställaren för att rättslig grund finns för personuppgiftsbehandlingarna som omfattas av upphandlingen.

- ansvarar beställaren för att informationsklassa informationsmängderna (inklusive personuppgifternas skyddsvärde) som upphandlingen om omfattar för att säkerställa att rätt säkerhetsnivå kravställs.
- ansvarar beställaren för att säkerställa att upphandlingen kravställs på ett sätt att dataskyddsförordningens krav efterlevs.
- ansvarar beställaren för att reglera personuppgiftsansvaret med upphandlad leverantör.
  - självständigt personuppgiftsansvar regleras i huvudavtalet,
  - gemensamt personuppgiftsansvar genom datadelningsavtal
  - biträdesförhållande genom personuppgiftsbiträdesavtal.
- ansvarar beställaren för att säkerställa att de tekniska och organisatoriska säkerhetsåtgärder som krävs implementeras, följs upp och vid behov åtgärdas utifrån samverkan med berörda nämnder.

## Personal

Varje gemensamt personuppgiftsansvarig nämnd ansvarar för att nämndens personal hanterar personuppgifterna som behandlas i enligt dataskyddslagstiftningens bestämmelser. Det innefattar att personalen ska ha tillräcklig kompetens för att hantera personuppgifterna på ett lagenligt och säkert sätt.

## De registrerades rättigheter

Varje gemensamt personuppgiftsansvarig nämnd ansvarar för att säkerställa att en registrerads inkomna begäran, att fullföra sina rättigheter, handläggs sakligt, effektivt och inom utsatt tid.

Den nämnd som mottagit begäran ska hantera begäran för sin räkning. I det fall begäran rör även andra personuppgiftsansvariga nämnders behandling, ska den nämnd som mottagit begäran informera övriga nämnder om att begäran inkommit.

I det fall en registrerad begär skadestånd för en gemensam personuppgiftsbehandling har varje personuppgiftsansvarig nämnd en skyldighet att utreda om det finns någon grund för skadestånd.

Kommunstyrelsen kan efter önskemål från berörda nämnder handlägga ärendet om det är en process som kommunstyrelsen ansvarar för.

# Ansvarsfördelning internt biträdesförhållande

Vid ett internt biträdesförhållande mellan nämnderna inklusive Djursholms AB i Danderyds kommun gäller följande.

## Behandlingsregister vid internt biträdesförhållande

Behandlingsregistret säkerställer att interna biträdesrelationer dokumenteras.

- Den personuppgiftsansvariga nämnden har ansvaret för att i samverkan med biträdet i behandlingsregister ange om personuppgiftsbehandlingen innebär ett internt biträdesförhållande och i mellan vilka nämnder biträdesrelationen föreligger.

## Risk- och konsekvensanalys vid internt biträdesförhållande

- Den personuppgiftsansvariga nämnden ansvarar för att säkerställa att konsekvensbedömning artikel 35 dataskyddsförordningen genomförs, uppdateras och följs upp samt att förteckna den i systemet för personuppgiftsbehandlingar.
- Den personuppgiftsansvariga nämnden ansvarar för att vidta de tekniska och organisatoriska säkerhetsåtgärder som krävs utifrån dels personuppgiftsbehandlingens artikel, dels vad konsekvensbedömningen visar.
- Den biträdande nämnden ansvarar för att samarbeta vid arbetet med risk- och konsekvensbedömning.

## Förhandssamråd vid internt biträdesförhållande

- Personuppgiftsansvarig nämnd ansvarar för att samordna handläggning, beslut och begäran om förhandssamråd samt att säkerställa ett genomförande av förhandssamrådet.
- Biträdande nämnd, i den mån denne berörs, ansvarar för att samarbeta med den personuppgiftsansvariga nämnden vid förhandssamrådet.

## Personuppgiftsincidenter vid internt biträdesförhållande

- Biträdande nämnd ansvarar för att informera personuppgiftsansvarig nämnd om anmäld personuppgiftsincident.
- Biträdande nämnd ansvarar för att efterleva personuppgiftsansvarigs instruktioner med anledning av inträffad incident.

### Revision och tillsyn vid internt biträdesförhållande

- Personuppgiftsansvarig nämnd kan initiera revision och tillsyn gentemot den nämnd som är personuppgiftsbiträde.
- Personuppgiftsansvarig nämnd är kontaktperson vid tillsyn av Dataskyddsombudet och/eller Integritetsskyddsmyndigheten.

### Upphandling och implementering vid internt biträdesförhållande

- Vid upphandling som omfattar internt biträdesförhållande ansvarar beställaren för att biträdet involveras i den mån det är nödvändigt för att säkerställa att dataskyddsförordningens krav efterlevs.

### Tekniska och organisatoriska säkerhetsåtgärder vid internt biträdesförhållande

- Personuppgiftsansvarig nämnd ansvarar för att klargöra vilka tekniska och organisatoriska säkerhetsåtgärder som krävs av biträdet.
- Biträdet ansvarar för att säkerställa de tekniska och organisatoriska säkerhetsåtgärderna som personuppgiftsansvarig ställer samt att påtala bister och felaktigheter.

### De registrerades rättigheter vid internt biträdesförhållande

- Enskild kan inkomma med begäran om fullgörande av sin rättighet till biträdet
- Alla nämnder ansvarar oaktat hur begäran inkommit för att säkerställa handläggning av enskilds begäran för sin nämnds räkning.
- Vid begäran om fullgörande av enskilds rättighet ansvarar personuppgiftsansvarig nämnd för handläggningen och biträdet biträder handläggningen.

## Kamerabevakning

Kamerabevakningslagen ålägger den personuppgiftsansvariga att fullgöra kraven i dataskyddslagstiftningen. Då frågan om kamerabevakning kan initieras från fler olika håll ansvarar den nämnd som initierar kamerabevakning för att tillsammans med personuppgiftsansvarig nämnd säkerställa att dataskyddslagstiftningens krav efterlevs.