Policy för informationssäkerhet och dataskydd

Diarienummer	Senast uppdaterad	Beslutsinstans	Ansvarig processägare
KS 2019/0428	2021-03-22 § 43	Kommunfullmäktige	Säkerhetschef

Dokumentets syfte

I Policy för informationssäkerhet och dataskydd fastställs grunderna för kommunens arbete med informationssäkerhet och dataskydd.

Dokumentet gäller för

Policy för informationssäkerhet och dataskydd gäller för samtliga nämnder och kommunala bolag.

Innehållsförteckning

Syfte och mål för informationssäkerhets- och dataskyddsarbetet

Policy för informationssäkerhet och dataskydd lägger grunden för Danderyds kommuns arbete med informationssäkerhet och dataskydd. De principer och regler som fastställs är styrande inom samtliga delar av kommunens verksamhet. Nämnderna har inte möjlighet att besluta om lokala avvikelser.

Informationssäkerhetsarbetets mål är för det första att kommunens information alltid ska vara tillgänglig där den behövs, för det andra att det alltid ska gå att lita på att informationen inte är manipulerad eller förstörd, för det tredje att informationen endast är tillgänglig för personer som är behöriga att få ta del av den, och för det fjärde att det ska gå att följa hur och när informationen har hanterats och kommunicerats.

Dataskyddsarbetets mål, utöver vad som gäller för informationssäkerheten, är att de personuppgifter som kommunen hanterar ska behandlas i enlighet med dataskyddslagstiftningen, varav Allmänna dataskyddsförordningen (EU) 2016/679 (DSF) utgör det centrala regelverket.

Informationssäkerhetsarbetet och dataskyddsarbetet bör samordnas då ett gott informationssäkerhetsarbete är en förutsättning för att följa dataskyddslagstiftningen.

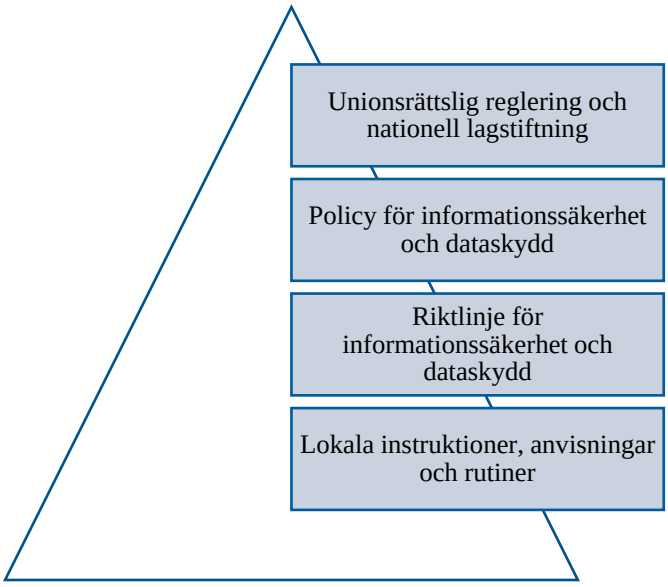
Styr- och stöddokumentshierarki

Kommunens hantering av information och personuppgifter är normbunden dels av den nationella rätten, dels av den unionsrättsliga regleringen bestående av EU:s rättsakter och EU-domstolens praxis.

Inom kommunens organisation bygger efterlevnaden av dessa regler på att styr- och stöddokument beslutas på lämplig nivå.

Policy för informationssäkerhet och dataskydd lägger grunden för Danderyds kommuns arbete med informationssäkerhet och dataskydd. Som ett led i uppgiften att leda och samordna nämndernas verksamheter ska kommunstyrelsen anta riktlinjer för säkerhet vilka reglerar hur personuppgifter ska behandlas och hur informationssäkerheten ska upprätthållas. Syftet med riktlinjerna ska vara att ge nämnderna förutsättningar för att efterleva nationell lagstiftning och unionsrättslig reglering.

I sista led ska varje nämnd vid behov införa anvisningar och rutiner för att informationssäkerhetsarbetet och behandlingen av personuppgifter, i varje konkret fall, ska kunna anpassas till de specifika förutsättningar som gäller inom respektive förvaltning.



Pyramid som illustrerar hierarkin för styr- och stöddokument.

Ansvarsfördelningen för informationssäkerheten

På samma sätt vad gäller dataskyddet är varje nämnd ansvarig för att tillräckliga åtgärder vidtas för att den information som nämnden ansvarar för hanteras på ett säkert sätt. Detta arbete ska vara långsiktigt, kontinuerligt och omfatta hela verksamheten och alla informationstillgångar som hanteras. Personuppgifter utgör en typ av informationstillgång. Samtliga anställda ska få fortlöpande utbildning för att förstå hur informationssäkerhetsarbetet fungerar. Informationssäkerheten ska utgöra en löpande del i riskhanteringsarbetet. Utgångspunkten är att information utgör en värdefull tillgång.

Personuppgiftsansvaret

Dataskyddsförordningen stadgar att ansvaret är knutet till den som är personuppgiftsansvarig. Det innebär att det är kommunens nämnder som själva har det allra yttersta ansvaret för att personuppgiftsbehandlingen i varje enskilt fall utförs i enlighet med förordningens regler och principer. Kommunfullmäktige eller ett utskott är inte personuppgiftsansvarig. En annan nämnd kan behandla personuppgifter för annan nämnds vägnar och blir därmed ett personuppgiftsbiträde (biträdesnämnd).

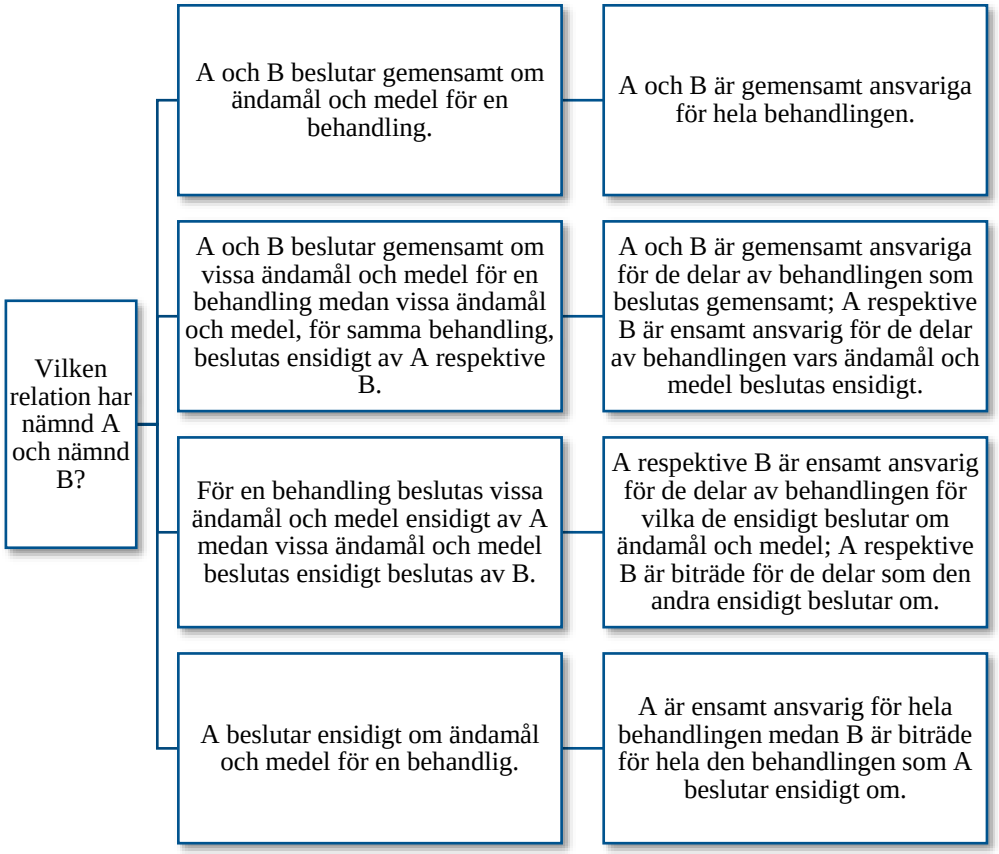
För att skyddet av den enskildes personuppgifter ska förverkligas i praktiken måste varje nämnd vidta lämpliga organisatoriska åtgärder och avsätta erforderliga personalresurser.[1] En korrekt hantering av personuppgifter ska vara en integrerad del i det dagliga arbetet på kommunens förvaltningar. Samtliga anställda ska få fortlöpande utbildning för att förstå hur dataskyddsarbetet fungerar.

[1] Tjänstemannaorganisationen regleras i riktlinje för säkerhet.

I personuppgiftsansvaret ingår att utse ett dataskyddsombud för den egna verksamheten.

Fördelning av personuppgiftsansvaret vid interna biträdesrelationer och definition av behandling

Av artikel 26 (DSF) följer att personuppgiftsansvaret kan vara gemensamt för det fall att två aktörer gemensamt fastställer ändamålen med och medlen för behandlingen. Europeiska dataskyddsstyrelsen (EDPS) har genom meddelade riktlinjer klargjort hur dataskyddsförordningens regler ska tillämpas i detta hänseende och vid biträdesrelationer.[2] I enlighet med riktlinjerna ska följande princip gälla för fördelning av personuppgiftsansvaret vid gemensamt personuppgiftsansvar och interna biträdesrelationer i Danderyds kommun.



Det är respektive nämnd som avgör för vilka behandlingar den är personuppgiftsansvarig för. Uppstår fråga om gemensamt ansvar för behandling ska berörda nämnder samråda för att lösa gränsdragningsfrågor.

Personuppgiftsansvarig nämnd är skyldig att meddela annan nämnd med vilken biträdesrelation föreligger. Biträdesnämnden registrerar biträdesrelationen i det egna behandlingsregistret enligt artikel 30 (DSF). Personuppgiftsansvarig nämnd ansvarar för att underrätta biträdesnämnden

[2] EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725 och Guidelines07/2020ontheconceptsofcontrollerand processor in the GDPR.

om biträdesrelation upphört, varefter biträdesnämnden kan ta bort behandlingen ur det egna behandlingsregistret.

Enligt artikel 4.2 (DSF) definieras en behandling som en åtgärd eller kombination av åtgärder. Av EDPS riktlinjer följer att en kombination av behandlingar inte bör delas upp som separata behandlingar om de, utifrån den registrerades perspektiv, bildar en enhet. En sådan tillämpning underlättar för den registrerade att bevaka sina rättigheter i och med att behandlingsregistret blir lättare att förstå. Det sagda innebär att rekvisitet behandling ska ges en övergripande processorienterad tolkning när så är möjligt. Personuppgiftsansvariga nämnder ska sträva efter att begreppet ges en enhetlig tillämpning.

Reglering av interna biträdesrelationer

Av artikel 28.3 (DSF) följer att när uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras, vilket kan genomföras med en rättsakt i enlighet med nationell lagstiftning. Kommunens rätt att meddela föreskrifter följer av 14 kap regeringsformen (1974:152) och 1 kap 3 § kommunallagen (2017:725). I enlighet därmed föreskrivs följande när en nämnd (biträdesnämnd) behandlar personuppgifter för annan nämnds räkning (personuppgiftsansvarig nämnd).

1. Förutsättningar för en biträdesnämnds behandling av personuppgifter följer av kommunens styrdokument för informationssäkerhet och dataskydd, respektive nämnds dokumenthanteringsplaner och personuppgiftsansvarig nämnds behandlingsregister som förs enligt artikel 30 (DSF).

2. Föremål för behandlingen, dess art och ändamål, typen av personuppgifter samt kategorier av registrerade anges i den personuppgiftsansvariga nämndens behandlingsregister enligt artikel 30 (DSF).

3. Behandlingens varaktighet pågår under den tid behandlingen finns intagen i personuppgiftsansvarig nämnds behandlingsregister enligt artikel 30. Personuppgiftsansvarig nämnd är skyldig att meddela uppgifterna till biträdesnämnden som i sin tur intar dem i det egna behandlingsregistret. Personuppgiftsansvarig nämnd ansvarar vidare för att underrätta biträdesnämnden om biträdesrelation upphört. Biträdesnämnden kan därefter ta bort behandlingen ur det egna behandlingsregistret.

4. Biträdesnämnden är enligt dataskyddsförordningen skyldig att behandla personuppgifter i enlighet med personuppgiftsansvarig nämnds instruktioner. Denna skyldighet fullgörs genom att biträdesnämnden följer kommunens antagna styrdokument gällande informationssäkerhet och dataskydd, gällande dokumenthanteringsplan och personuppgiftsansvarigs dataskyddsregister som förs enligt artikel 30 (DSF). Eventuella ytterligare instruktioner från personuppgiftsansvarig nämnd ska vara i enlighet med kommunens styrdokument för informationssäkerhet och dataskydd.

5. Biträdesnämnden är skyldig att behandla uppgifterna i enlighet med dataskyddsförordningens krav om konfidentialitet. Denna skyldighet

fullgörs genom att biträdesnämnden följer gällande offentlighets- och sekretesslagstiftning samt kommunens styrdokument för informationssäkerhet och dataskydd.

6. Biträdesnämnden ska vidta alla åtgärder som krävs enligt artikel 32 (DSF) om säkerhet i samband med behandlingen.

7. Biträdesnämnden ska respektera de villkor som avses i artikel 28.2 och 28.4 för anlitande av ett annat personuppgiftsbiträde.

8. Biträdesnämnden ska så långt det är möjligt hjälpa den personuppgiftsansvariga nämnden att fullgöra skyldigheten att svara på begäran om utövande av den registrerades rättigheter i enlighet med kapitel III (DSF).

9. Biträdesnämnden ska bistå personuppgiftsansvarig nämnd med att säkerställa att skyldigheterna enligt artiklarna 32–36 (DSF) fullgörs.

10. Biträdesnämnden ska på den personuppgiftsansvariga nämndens begäran radera eller återlämna alla personuppgifter efter det att tillhandahållandet av behandlingstjänster har avslutats och radera befintliga kopior. Detta gäller såvida inte lagring av personuppgifterna krävs enligt lagstiftning eller kommunens styrande dokument.

11. Biträdesnämnden ska ge personuppgiftsansvarig nämnd tillgång till all information som krävs för att visa att biträdesnämndens skyldigheter har fullgjorts. Biträdesnämnden ska vidare möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvariga nämnden eller av en annan revisor som bemyndigats av den personuppgiftsansvariga nämnden. Biträdesnämnden ska omedelbart informera personuppgiftsansvarig nämnd om den anser att en instruktion strider mot dataskyddsförordningen eller mot andra av unionens eller dataskyddslagstiftningens skyddsbestämmelser.

Rättslig grund för behandling av personuppgifter

Tillämpningen av dataskyddsförordningen bygger i grunden på två steg. För det första måste det finnas ett rättsligt stöd för att behandlingen över huvud taget ska få ske. De rättsliga grunderna framgår av artikel 6 (DSF). För det andra ska behandlingen i övrigt utföras i enlighet med de principer som framgår av artikel 5 (DSF).

Att det enligt förordningen finns en rättslig grund för behandlingen är dock i sig inte tillräckligt för att behandlingen ska få ske. Uppgiften att behandla personuppgifter måste därutöver vara fastställd i enlighet med unionsrätten eller den nationella rätten. Det innebär att den måste följa av lag eller annan författning, av kollektivavtal eller av beslut som meddelats med stöd av lag eller annan författning.

Danderyds kommun kan fatta beslut som skapar rättslig grund för behandling som utgör ett allmänt intresse och som behöver utföras men som inte följer direkt av lag, annan författning eller av kollektivavtal. Sådan

rättslig grund kan endast skapas genom beslut i kommunfullmäktige i form av reglementen, policyer eller andra former av styrdokument.

Av förordningen följer samtidigt att behandling kan ske om någon annan rättslig grund föreligger. Ett sådant exempel är om den enskilde har samtyckt till behandlingen för ett eller flera specifika ändamål. I enlighet med den ovan nämnda styr- och stöddokumentshierarkin kan kommunen föreskriva hur sådant samtycke ska inhämtas och utformas.

Webbpublicering av personuppgifter med anledning av ett allmänt intresse

En av de lagliga grunderna för behandling av personuppgifter är ”allmänt intresse” (art 6.e DSF). På Danderyds kommuns officiella hemsidor publiceras viktig och värdefull information som utgör ett allmänt intresse eftersom den är av vikt för kommunens invånare i och med att den främjar den demokratiska processen.

Enligt 8 kap 10–11 §§ kommunallagen (2017:725) kan kommunens elektroniska anslagstavla innehålla justerade protokoll i den utsträckning kommunen bestämmer det. Därutöver kan följande handlingar läggas ut: tillkännagivanden om styrelsens och övriga nämnders sammanträden samt beslutsunderlag inför fullmäktiges, styrelsens och övriga nämnders sammanträden. Webbpublicering av kallelser, protokoll och beslutsunderlag har därmed rättslig grund och utgör samtidigt ett allmänt intresse. Av lydelsen följer dock att det ankommer på kommunen att bestämma i vilken utsträckning webbpublicering ska ske. Således ska varje nämnd i Danderyds kommun besluta i vilken utsträckning som justerade protokoll, kallelser och beslutsunderlag ska publiceras på hemsidan. Personuppgiftsansvarig nämnd bär dock alltid ansvaret för att kontrollera att sådan publicering görs i enlighet med de regler och principer som följer av dataskyddslagstiftningen.

Utöver kallelser, protokoll och beslutsunderlag kan personuppgifter publiceras på kommunens officiella hemsidor i det fall det gäller information och nyheter som är av vikt för kommunens invånare, webbsändning, inklusive eftersändning av kommunfullmäktiges sammanträde samt Danderyds kommuns dialogforum.

Av det sagda följer att personuppgifter får publiceras på webben, det vill säga hemsida och sociala medier, i följande sammanhang med den lagliga grunden allmänt intresse:

1. Protokoll, kallelser och beslutsunderlag i den mån respektive nämnd har beslutat om det.
2. Information och nyheter som är av vikt för kommunens invånare.
3. Webbsändning och eftersändning av kommunfullmäktiges sammanträden.