BILAGA 3

Motivering till förslagen avseende kategori P GDPR och dataskyddslagen

1. Beslut avseende tillgodoseende av rättigheter – GDPR artikel 15-21

   Motivering: Tillgodoseende av rättigheter ska ske utan onödigt dröjsmål, dock inom en månad. Rent lagtekniskt finns möjlighet att förlänga fristen att tillgodose rättigheter med två ytterligare månader. Det är i individens intresse att få sina rättigheter tillgodosedda utan dröjsmål, det är även i individens intresse att en begränsad personkrets tar del av rättighetsbegäran. Därför är det lämpligt att ärenden rörande tillgodoseende av individers rättigheter behandlas av tjänsteperson som handlägger ärendet där den registrerades personuppgifter figurerar.

2. Adekvansbeslut avseende tekniska och organisatoriska åtgärder för att säkerställa regelefterlevnad – GDPR artikel 24-25

   Motivering: Beslut avseende adekvans rörande tekniska och organisatoriska åtgärder för att säkerställa efterlevnaden av GDPR kräver ett omfattande arbete där flertalet experter är delaktiga. Bland annat behövs teknisk och juridisk kompetens vid bedömningen, men även kunskap om den process/behandling som genomförs behövs för att kunna avgöra om åtgärder är adekvata och proportionella. För att säkerställa att beslutet är tillräckligt ska även dataskyddsombudets vägledning inhämtas. Dataskyddsombudet har dock inte beslutanderätt utan kan enbart ge rekommendation. För att ingen enskild handläggare ska belastas med beslut där den kommunala myndigheten bär det slutgiltiga ansvaret bör det vara en högt uppsatt tjänsteperson inom förvaltningen som får delegation att fatta beslut.

3. Adekvansbeslut avseende inbyggda säkerhetsåtgärder i samband med upphandling – GDPR artikel 25

   Motivering: I samband med upphandlingar, särskilt i samband med upphandlingar av IT-system, behöver leverantören garantera det som kallas dataskydd som standard och inbyggt dataskydd. Då detta är något som ingår i upphandlingsprocessen är det den chef som är ansvarig för en given upphandling som ska avgöra om de åtgärder som tagits av leverantören är adekvata och proportionella. Dataskyddsombudet ska höras.

4. Beslut avseende ansvarsfördelning vid gemensamt personuppgiftsansvar – GDPR artikel 26

   Motivering: Personuppgiftsansvar under GDPR kan vara delat i fall som gäller främst samarbetsavtal mellan nämnder i olika kommuner. I dessa fall behöver det tydliggöras vem som har vilka skyldigheter gentemot de registrerade. Givet den principiella vikten av denna typ av förhandling/beslut bör beslutet fattas på den högsta tjänstemannanivån. Förvaltningschefen föreslås därför vara delegat.

5. Beslut avseende tekniska och organisatoriska åtgärder vidtagna av personuppgiftsbiträde – GDPR artikel 28

   Motivering: I samband med upphandlingar, särskilt i samband med upphandlingar av IT-system, ska det ställas krav på de tekniska och organisatoriska säkerhetsåtgärder som leverantören vidtar vid utförande av uppdrag som innebär personuppgiftsbehandling å nämndens vägnar. Då detta är något som ingår i upphandlingsprocessen är det den chef som är ansvarig för en given upphandling som ska avgöra om de åtgärder som vidtagits av leverantören är adekvata och proportionella. Dataskyddsombudet ska höras.

6. Tecknande av personuppgiftsbiträdesavtal – GDPR artikel 28

   Motivering: I samtliga situationer där en leverantör utför ett uppdrag åt nämnden behöver nämnden specificera vad leverantören ska genomföra för behandling. Nämnden är i egenskap av personuppgiftsansvarig skyldig att ta fram avtal och instruktion till personuppgiftsbiträdet. Då ett personuppgiftsbiträdesavtal i essens är en bilaga till tjänsteavtal och tecknande av tjänsteavtal är delegerat till tjänsteperson är det även lämpligt att denna fråga delegeras till samma tjänsteperson som varit ansvarig för att teckna tjänsteavtalet.

7. Instruktion till personuppgiftsbiträde – GDPR artikel 28
   Motivering: Instruktioner till personuppgiftsbiträde behöver ges vid vissa tillfällen, till exempel vid avtalets upphörande då biträdet antingen ska föra över till personuppgiftsansvarig eller radera de personuppgifter som de behandlar på uppdrag av den personuppgiftsansvarige. Även vid personuppgiftsincidenter kan det vara nödvändigt att instruera personuppgiftsbiträdet hur detta ska agera. Instruktion till personuppgiftsbiträdet kan även vara nödvändigt eller skäligt vid andra tillfällen. Det behöver således finnas en person i nämndens förvaltning som har detta mandat. Föreslaget är att samma person som tecknat avtalet med personuppgiftsbiträdet även är ansvarig för instruktioner till detsamma.

8. Kontaktperson gentemot tillsynsmyndigheten då tillsynsmyndigheten initierar kontakt med nämnden – GDPR artikel 31

   Motivering: Det åligger nämnden i egenskap av personuppgiftsansvarig att samarbeta med tillsynsmyndigheten vid tillsynsmyndighetens utförande av sina uppgifter. Detta innebär att nämnden behöver utse en person som agerar kontaktpunkt åt tillsynsmyndigheten vid dessa tillfällen för att underlätta samarbetet med tillsynsmyndigheten. Förslagsvis bör myndighetens kontaktperson vara förvaltningschefen vid dessa tillfällen eftersom myndighetens uppgifter kan omfatta samtliga behandlingar som nämnden är ansvarig för.

9. Adekvansbeslut avseende tekniska och organisatoriska säkerhetsåtgärder vidtagna för att minska risken för och vid personuppgiftsincidenter vid behandling – GDPR artikel 32

Motivering: Nämnden har i egenskap av personuppgiftsansvarig en skyldighet att säkerställa att det finns adekvata säkerhetsåtgärder på plats, tekniska såväl som organisatoriska, för att förebygga personuppgiftsincidenter samt för att begränsa skada av personuppgiftsincidenter när dessa uppstår. I och med att ansvaret är organisatoriskt bör delegat vara en tjänsteperson i hög beslutsfattande ställning. Denna tjänsteperson föreslås vara förvaltningschefen då flera delar av förvaltningen behöver samverka för att säkerställa att de organisatoriska och tekniska säkerhetsåtgärderna är adekvata och proportionella.

10. Anmälan av personuppgiftsincident till tillsynsmyndigheten – GDPR artikel 33

    Motivering: Anmälan av personuppgiftsincidenter till tillsynsmyndigheten åligger den personuppgiftsansvarige organisationen. En personuppgiftsincident måste anmälas till tillsynsmyndigheten inom 72 timmar från dess upptäckt. Således är det inte möjligt att invänta nämndens beslut vid anmälan av personuppgiftsincident till tillsynsmyndigheten. Det föreslås att förvaltningschefen ska anmäla personuppgiftsincidenter till tillsynsmyndigheten då flera delar av myndigheten typiskt sett behöver involveras när en personuppgiftsincident har uppstått. Uppgiften kan också vidaredelegeras.

11. Beslut avseende information till registrerade i samband med personuppgiftsincident – GDPR artikel 34

    Motivering: I samband med en personuppgiftsincident är det den personuppgiftsansvariges skyldighet att informera registrerade som drabbats av incidenten. Detta förutsatt att incidenten sannolikt leder till hög risk för den registrerades fri- och rättigheter. Det finns inget som hindrar den personuppgiftsansvarige att informera registrerade även vid mindre omfattande incidenter. Då informationen till registrerade ska levereras utan onödigt dröjsmål är det lämpligt att en tjänsteperson gör bedömningen avseende huruvida registrerade ska kontaktas eller ej. Beslutet bör fattas på en hög nivå då ansvaret är organisatoriskt. Därför föreslås förvaltningschefen vara delegat.

12. Beslut avseende genomförande av konsekvensbedömning – GDPR artikel 35

    Motivering: Den personuppgiftsansvarige har en skyldighet att genomföra en så kallad konsekvensbedömning, det vill säga en riskanalys, inför att behandling som kan innebära hög risk för den registrerades fri- och rättigheter genomförs. Ett typexempel på sådan behandling är videoövervakning av allmän plats. Givet att beslutet att genomföra konsekvensbedömning är ett organisatoriskt ansvar bör bedömningen av huruvida konsekvensbedömning ska genomföras eller ej antingen beslutas av högt uppsatta tjänstepersoner i förvaltningen. Föreslaget är att förvaltningschefen ges delegation i frågan.

13. Yttrande avseende möjligheterna att påbörja behandling efter genomförd konsekvensbedömning – GDPR artikel 35

Motivering: Yttrande av denna typ bör göras av representant både från förvaltningen och från dataskyddsombudet i egenskap av oberoende granskare av nämndens regelefterlevnad, då frågan avser huruvida den personuppgiftsansvarige ska genomföra en högriskbehandling eller ej. Ärenden av denna typ är av central vikt för registrerades fri- och rättigheter och är således en renodlad demokratifråga. Ärendet ska således beslutas på nämndnivå och föredras av förvaltningschefen samt av dataskyddsombudet.

14. Beslut om kontaktperson gentemot tillsynsmyndigheten vid förhandssamråd – GDPR artikel 36

    Motivering: Istället för att fatta beslut att genomföra behandling eller ej genomföra behandling i ärenden under punkt 16 ska nämnden besluta att begära förhandssamråd om de vill genomföra behandling trots att genomförandet kommer innebära hög risk för registrerade som omfattas av behandlingen. Kontaktperson vid förhandsamrådet föreslås vara förvaltningschefen i enlighet med förslaget i punkt 8.

15. Yttrande avseende möjligheterna att genomföra behandling efter förhandssamråd med tillsynsmyndigheten – GDPR artikel 36

    Motivering: Motiveringen är densamma som under 14.

16. Yttrande avseende utnämnande av dataskyddsombud – GDPR artikel 37

    Motivering: Dataskyddsombudet ska vara självständigt i utförande av sina arbetsuppgifter och ska rapportera till den personuppgiftsansvariges högsta förvaltningsnivå, det vill säga nämnden. Utnämnande av Dataskyddsombudet ska därför göras av nämnden. Förvaltningschefen i egenskap av högste tjänsteman inom förvaltningen ska uppdras att föreslå kandidater för nämnden.

17. Beslut att bestrida beslut från tillsynsmyndighet – GDPR artikel 57

    Motivering: Beslut att bestrida tillsynsmyndighetens beslut bör fattas på en så hög nivå som möjligt, då detta ofta är principiellt viktiga beslut samt även beslut av betungande ekonomisk natur. Eftersom besluten har en överklagandefrist finns risken att kultur- och fritidsnämnden ej hinner fatta beslut i denna typ av ärende. Det föreslås därför att kultur- och fritidsnämndens ordförande ska utses till delegat, i egenskap av den främste företrädaren för kultur- och fritidsnämnden. Om tid finns saknas hinder att lyfta frågan till kultur- och fritidsnämnden.

18. Ändringsbeslut avseende tillgodoseende av rättigheter efter överklagande – Dataskyddslagen 7 kap. 2 §

    Motivering: I de fall förvaltningen har beslutat att den enskilde ej har rätt att utöva en viss rättighet under GDPR är det möjligt för den enskilde att överklaga detta beslut. Det finns då under dataskyddslagen möjlighet att ändra beslutet till den enskildes förmån. För att undvika jäv i beslutsfattandet bör denna typ av ändringsbeslut fattas av en tjänsteperson i

högre beslutsfattande ställning än den som fattade det initiala beslutet. Delegaten föreslås därför vara förvaltningschefen.