Bilaga - Pris
Upphandling system för förvaltarenheten, Stockholms stad

Instruktion: Anbudsgivare anger pris i de grå rutorna

Pris för systemet

Pris för tillgång och nyttjanderätt till systemet för Stockholms stad, Förvaltarenheten, enligt kravställd funktionalitet, avser nya versioner och uppdateringar, support och underhåll och SLA. Antalet användare kan variera under avtalsperioden.

	Pris	Enhet	summa 4 år	
Pris per år, år 1-4	- kr	kr per år	- kr	pris ingår i anbudspris
Pris per år, år 5-8	- kr	kr per år	- kr	pris ingår i anbudspris
summa			**- kr**	

Priser Införande

Beskrivning	Antal	Pris	Enhet	Summa	
Införandekostnad enligt förutsättningar i kravspecifikationen (innefattar integrationer, driftsättning, initiala utbildningsinsatser samt andra tillkommande engångskostnader i samband med införandet)	1	- kr	kr	- kr	pris ingår i anbudspris
Summa				**- kr**	

Priser optioner

Beskrivning	Fiktivt antal timmar	Pris	Enhet	Summa	
		Löpande kostnader			
1. Konsultstöd, utbildning, för extra utbildningsinsatser	20	- kr	kr per timme	- kr	pris ingår i anbudspris
2. Konsultstöd som har god kännedom om tjänstens utformning och som kan systemets olika delar utifrån uppbyggnad exempelvis behörigheter, konfigurering, införande av ny funktionalitet etc.	20	- kr	kr per timme	- kr	pris ingår i anbudspris
3. Konsultstöd med kompetens inom övergripande områden, som kan anlitas vid behov, exempelvis: IT, säkerhet och integrationer, som är kopplade till tjänstens utformning m.m.	20	- kr	kr per timme	- kr	pris ingår i anbudspris
Summa				**- kr**	

Anbudspris

Engångsavgifter	- kr	
Löpande avgifter	- kr	
Totalt anbudspris för införande och avgifter för hela avtalstiden	**- kr**	**pris som används för utvärdering**

Stockholms stad

Riktlinje för informationssäkerhet i Stockholms stad

Beslutad av kommunfullmäktige 2022-02-21

Om denna riktlinje

Denna riktlinje är en del av Stockholms stads kvalitetsprogram och reglerar arbetet med informationssäkerhet inom samtliga nämnder och bolag (nedan kallade *nämnder och styrelser*) i Stockholms stad (nedan benämnt staden). Området informationssäkerhet berörs även i styrdokument rörande säkerhet.

Denna riktlinje är en del av Stockholms stads kvalitetsprogram och reglerar arbetet med informationssäkerhet inom samtliga nämnder och bolag i Stockholms stad.

Riktlinjen består dels av övergripande mål och principer för informationssäkerhetsarbetet och som beskrivs i detta dokument, dels av ett antal fördjupade tillämpningsanvisningar inom särskilda områden, exempelvis informationsklassning eller åtkomsthantering.

Riktlinjen beslutas av kommunfullmäktige och utgör en central del i stadens ledningssystem för informationssäkerhet.

Tillämpningsanvisningar beslutas av kommunstyrelsen eller av den kommunstyrelsen delegerat rätten att fatta beslut om dessa till.

Bakgrund och syfte med riktlinjen

Stadens kvalitetsarbete syftar till att öka kvaliteten i genomförandet av det kommunala uppdraget och samtidigt möta dagens och morgondagens utmaningar. Det ställer krav på att staden utför ett grundläggande och systematiska informationssäkerhetsarbete i alla sina verksamheter. Denna riktlinje anger kommunfullmäktiges direktiv för detta arbete. Arbetet ska i sin tur bidra till att staden upprätthåller trygghet och förtroende hos medborgare, näringsliv och besökare, men också att lagar, förordningar och riktlinjer efterlevs.

Dagens informationssamhälle har lett till att grundläggande samhällsfunktioner är beroende av information i digitala tjänster. Detta beroende innebär i sin tur risker. Därför har kraven på skydd för information skärpts avsevärt genom lagstiftning, exempelvis dataskyddförordningen och NIS-direktivet[1] samt regeringens strategi på nationell nivå. Både stadens ambitioner och svensk lagstiftning förutsätter en ändamålsenlig informationssäkerhet i stadens nämnder och styrelser.

1 NIS (Directive on Security on Network and Information Systems) är ett EU-direktiv som implementeras genom svensk lagstiftning i Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster. Lagen trädde i kraft 2018 och syftar till att uppnå en hög gemensam nivå av säkerhet i nätverk och informationssystem inom EU.

Stockholm har som ambition att genom digitalisering skapa bättre kvalitet i stadens tjänster, frigöra personalens tid, minska miljöpåverkan och uppnå en mer kostnadseffektiv handläggning av ärenden. Om informationen innehåller fel, inte går att komma åt eller hamnar i fel händer kan inte trygghet, effektivitet och innovation uppnås i samma utsträckning. Därför måste stadens nämnder och styrelser arbeta systematiskt med informationssäkerhet i sina verksamheter.

Definitioner

Informationssäkerhet är ett teknikneutralt begrepp vilket innebär skydd av information, oavsett om den är muntlig, pappersbunden eller digital. Med informationssäkerhet avses att rätt information ska finnas tillgänglig för rätt mottagare vid rätt tillfälle.

Skyddet avser därför att upprätthålla informationens:

- konfidentialitet
- riktighet
- tillgänglighet

Begreppet *konfidentialitet* ska ses i ett vidare perspektiv och omfattar både personlig integritet för enskilda och sekretess enligt offentlighets- och sekretesslagens mening, men även andra krav på att information inte ska komma obehöriga till del.

Med begreppet *riktighet* avses att information som hanteras ska vara oförvanskad och skyddad från otillåten manipulering. Dataskyddsförordningens grundläggande princip om riktighet har vidgat betydelsen av begreppet. Begreppet omfattar numera även att informationen ska vara riktig i den meningen att den är tillförlitlig och korrekt. Det innebär bland annat att rätt uppgifter hämtas från rätt datakälla för att användas i avsett syfte. Det innebär även att felaktiga uppgifter ska rättas vid behov.

Begreppet *tillgänglighet* omfattar, förutom tillgång till information vid en given tidpunkt, även tillgänglighet över tid kopplat till bevarande och gallringsplaner enligt arkivbestämmelser.

Likaså är *spårbarhet* en nödvändig del av informationssäkerhetsarbetet. Med spårbarhet menas möjligheten att i efterhand följa aktiviteter som är vidtagna med informationen, exempelvis att en person haft åtkomst till eller ändrat viss skyddsvärd information.

Dataskydd innebär skydd av personuppgifter enligt kraven i dataskyddsförordningen. Dataskydd är en del av informationssäkerhetsarbetet i staden.

Systematiskt informationssäkerhetsarbete är det arbete som ska utföras inom nämnder och styrelser för att skapa det skydd och den goda informationskvalitet som verksamheten behöver för att utföra sitt uppdrag. Arbetet utförs inom tre områden; organisatorisk säkerhet, it-säkerhet och fysisk säkerhet.

Organisatorisk säkerhet omfattar bland annat att roller, ansvar och arbetsuppgifter är definierade av verksamheten. Det omfattar även fastställda processer, rutiner och styrdokument som stödjer medarbetare att utföra informationssäkerhetsåtgärder i det dagliga linjearbetet.

It-säkerhet omfattar de tekniska åtgärder som ska vidtas som en följd av att viss information hanteras i en it- tjänst, till exempel virusskydd, tekniska filter mot bluff-mail och kryptering.

Fysisk säkerhet omfattar de fysiska åtgärder som ska vidtas som en följd av att information behöver skyddas, med exempel begränsat tillträde till vissa byggnader, säkerhetsskåp eller kylsystem för servrar.

It-tjänst används som samlingsnamn i riktlinjen och omfattar exempelvis it-system, it-tjänster, it-infrastruktur, it-plattformar, IoT (Internet of Things), molntjänster, sensorer, styrsystem (OT) och datakommunikation.

Tillämpning av standard för informationssäkerhetsarbetet

Stadens inriktning är att informationssäkerhetsarbetet inom nämnder och styrelser ska utgå från den internationella standarden SS-ISO/IEC 27001/2. Informationssäkerhetsarbetet ska alltid utföras med hänsyn tagen till stadens övergripande mål samt till nämnders och styrelsers egna verksamhetsuppdrag.

Informationssäkerhetsarbetet ska alltid utföras med hänsyn tagen till stadens övergripande mål samt till nämnders och styrelsers egna verksamhetsuppdrag.

Omfattning och avgränsningar för riktlinjen

Samtliga nämnder och styrelser i staden ska tillämpa denna riktlinje inklusive tillhörande tillämpningsanvisningar för all informationshantering. Dessa gäller för samtliga anställda, samt för externa uppdragstagare som leverantörer och konsulter.

Riktlinjen ska tillämpas i befintlig informationshantering och i samband med förändringar, utvecklingsarbete och upphandlingar.

Stockholms stads barn, elever och studerande i skolväsendet omfattas av regelverket i den utsträckning det är tillämpbart.

Avgränsning

Den verksamhet och informationshantering som träffas av säkerhetsskyddslagen omfattas inte av kraven i denna riktlinje. För sådan hantering gäller Säkerhetsskyddslagen samt av staden beslutade styrdokument för området.

Beskrivning av Stockholms stads ledningssystem för informationssäkerhet

Stadens ledningssystem för informationssäkerhet sätter ramarna för hur staden styr, genomför och följer upp informationssäkerhetsarbetet.

Ledningssystemet för informationssäkerhet består av flera delar. Dels av styrdokument som är stadsövergripande och gäller för samtliga verksamheter. Dels av lokalt framtagna styrdokument som enbart gäller för den egna verksamheten. En beskrivning av de stadsövergripande styrdokumenten följer nedan.

- Riktlinje för informationssäkerhet (detta dokument). Styrdokumentet anger kommunfullmäktiges direktiv för stadens informationssäkerhetsarbete.
- Riktlinjen kompletteras med tillämpningsanvisningar som detaljerar krav för olika delområden i informationssäkerhetsarbetet, exempelvis informationsklassning eller behörighetshantering. Tillämpningsanvisningarna beslutas var och en för sig av kommunstyrelsen eller av den kommunstyrelsen delegerat rätten att fatta beslut om dessa till.
- Metodstöd, handböcker, mallar, utbildningsmaterial och liknande som ger stöd för olika analyser och aktiviteter som ska utföras i nämnder styrelser.

En beskrivning av lokalt framtagna styrdokument följer nedan. Nämnder och styrelser ansvarar för att de lokala styrdokumenten upprättas för den egna verksamheten.

- En lokal anvisning som beskriver hur de övergripande reglerna för informationssäkerhetsarbetet tillämpas lokalt i den egna verksamheten (exempelvis hur den lokala informationssäkerhetsorganisationen ser ut, dess mandat och resurser, vem som ansvarar för att ta fram lokala styrdokument, hur arbetet följs upp med mera).
- Lokala styrdokument och informationssäkerhetsrutiner, exempelvis en incidentrutin, som är anpassade för specifika behov i verksamheten.

Riskbaserat informationssäkerhetsarbete

Verksamheten ska arbeta med att identifiera, bedöma och följa upp de informationssäkerhetsrisker som kan uppstå i verksamhetens informationshantering.

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska nämnder och styrelser ha ett riskbaserat förhållningssätt i sitt informationssäkerhetsarbete. Det innebär att verksamheten ska arbeta med att identifiera, bedöma och följa upp de informationssäkerhetsrisker som kan uppstå i verksamhetens informationshantering, exempelvis i linjeverksamheten eller hos externa leverantörer. Riskarbetet ska både genomföras tidigt i ett utvecklingsarbete så väl som i det löpande arbetet.

Ansvarsfördelning för informationssäkerhet

Nedan följer de övergripande principer för roller och ansvar som gäller för stadens informationssäkerhetsarbete. Ansvarsfördelningen beskrivs i detalj i tillämpningsanvisningen för roller och ansvar.

Ansvar för stadsgemensam styrning av informationssäkerhet

Ytterst är det *kommunfullmäktige* som ansvarar för de stadsövergripande direktiven för informationssäkerhetsarbetet genom denna riktlinje.

Kommunstyrelsen ansvarar för den strategiska ledningen och samordningen av det stadsövergripande informationssäkerhetsarbetet. Kommunstyrelsen fattar också beslut om tillämpningsanvisningar.

Ansvar för tillämpning av reglerna i nämnder och styrelser

Nämnder och styrelser ansvarar för att det bedrivs ett effektivt och ändamålsenligt informationssäkerhetsarbete i den egna verksamheten, samt att reglerna i denna riktlinje och tillhörande tillämpningsanvisningar tillämpas.

Förvaltnings- och bolagschef ansvarar för den operativa styrningen, resurstilldelningen och uppföljningen av det lokala informationssäkerhetsarbetet.

Samtliga medarbetare, och övriga som denna riktlinje gäller, exempelvis leverantörer och konsulter, ska följa gällande regler avseende informationssäkerhet och verka för en god säkerhetskultur.

Informationsägare

Informationsägare är den nämnd/styrelse som ansvarar för att den information som verksamheten hanterar är riktig och tillförlitlig samt ansvarar för hur informationen hanteras och sprids. Förvaltnings- eller bolagschef är nämndens/styrelsens operativa informationsägarrepresentant i linjen.

Informationsägaren ansvarar för att verksamhetens krav på informationssäkerhet fastställs genom informationsklassning. Informationsägaren ansvarar för att resultatet från informationsklassningen tas om hand och efterlevs. Det innebär exempelvis att tekniska säkerhetskrav från informationsklassningen kan överlämnas till den som förvaltar den tekniska

it-tjänsten, exempelvis en förvaltningsledare eller en it-leverantör, men att ansvaret för att de tekniska säkerhetskraven har implementerats aldrig kan överlämnas till en annan part.

Vägledande mål och principer

Nämnder och styrelser ska bedriva informationssäkerhetsarbetet på ett systematiskt och riskbaserat sätt och vägledas av följande mål och principer.

- Ansvaret för informationssäkerhet är känt och accepterat. Roller med ansvar för informationssäkerhet har ledningens stöd och mandat för att kunna utöva ansvaret.
- Säkerhetsnivå och inriktning för arbetet bygger på riskanalyser och informationsklassningar.
- All information och alla it-tjänster har en ägare. Ägare av informationen respektive ägare av it-tjänster ansvarar för att dessa skyddas i enlighet med kraven i denna riktlinje samt kraven från genomförd klassning och riskanalys.
- Rätt information finns tillgänglig för rätt mottagare vid rätt tidpunkt på ett spårbart sätt. Den princip som styr vilken information som en mottagare får tillgång till är att tillgång endast ges då arbetsuppgifterna motiverar det samt att sekretessregler tillåter det.
- Arbetet med dataskydd är integrerat i det generella informationssäkerhetsarbetet.
- Informationssäkerhetsarbetet i nämnder och styrelser är utformat så att det tar hänsyn till de skiftande krav, behov och lagstiftning som gäller i olika verksamheter.
- Det finns en positiv säkerhetskultur som uppmuntrar engagemang hos alla anställda och övriga som denna riktlinje gäller, och bidrar till att regler efterlevs och ständig förbättring av informationssäkerheten uppnås. Samtliga medarbetare genomgår årligen de obligatoriska utbildningar för informationssäkerhet som är beslutade.

Uppföljning

Stadens arbete med informationssäkerhet ska följas upp genom både interna granskningar och genom externa revisioner av oberoende part. Uppföljningen ska ske såväl inom samtliga nämnder och bolagsstyrelser som på stadsövergripande nivå. Stadens beslutade processer för internkontroll ska följas.

Stadens arbete med informationssäkerhet ska följas upp genom både interna granskningar och genom externa revisioner av oberoende part.

Fördjupade tillämpningsanvisningar

Denna riktlinje kompletteras av ett antal fördjupande tillämpningsanvisningar inom ett antal områden, exempelvis inom informationsklassning, identitet och åtkomst samt incidenthantering.

Riktlinje för informationssäkerhet i Stockholms stad

Dnr: 2021/866 | Utgivningsdatum: 21 februari 2022
Utgivare: Stadsledningskontoret | Kontakt: kommunstyrelsen@stockholm.se
Produktion: Blomquist Communication | Tryck: Åtta45 Tryckeri AB
Omslagsfoto: Lieselotte van der Meijs

start.stockholm

Stockholms stad

Tillämpningsanvisning för central it-infrastruktur och plattformar

Beskrivning av den centrala it-infrastrukturen och de plattformar som ska användas vid digitalisering i Stockholms stad

Beslutad av stadsdirektören 2023-04-11

Om tillämpningsanvisningen

I detta dokument beskrivs stadens centrala it-infrastruktur och plattformar på en övergripande nivå. Den centrala it-infrastrukturen och plattformarna är etablerade för att användas av stadens nämnder och styrelser och får inte dupliceras, om inte annat anges i detta dokument. Frågor om detta dokument och om mer detaljer kring den centrala it-infrastrukturen och plattformarna kan ställas till stadsledningskontoret, avdelningen för it och digitalisering på: Funktion.it@stockholm.se.

Version	Ändring	Datum
1.0	Första utgåva efter att kvalitetsprogrammet antagits. Ersätter tidigare riktlinje för stadens it-infrastruktur.	2023-04-11

Tillämpningsanvisning för central it-infrastruktur och plattformar
Dnr: KS 2022/1038
Beslutad av: Stadsdirektören
Beslutsdatum: 2023-04-11
Dokumentansvarig: Avdelningen för it och digitalisering
Kontakt: Funktion.it@stockholm.se
Dokumentet ersätter: Riktlinje för stadens it-infrastruktur

Innehåll

1 Inledning

I detta dokument beskrivs stadens centrala it-infrastruktur och plattformar på en övergripande nivå. Den centrala it-infrastrukturen och plattformarna är etablerade för att användas av stadens nämnder och styrelser och får inte dupliceras, om inte annat anges i detta dokument.

Kommunfullmäktige beslutade den 21 februari 2022 att anta Stockholms stads kvalitetsprogram (dnr 2021/866). Kvalitetsprogrammet gäller alla stadens nämnder och styrelser och är stadens styrande dokument för kvalitetsarbetet som omfattar ständiga förbättringar, innovation och digitalisering.

Av programmet framgår att stadens verksamheter behöver digitala lösningar som är kostnadseffektiva, stabila, långsiktigt hållbara och som möjliggör organisationsöverskridande samverkan. För att uppnå detta behövs gemensamma digitala lösningar som används av samtliga eller flera nämnder och styrelser. De omfattar infrastruktur och plattformar såsom gemensamt nätverk, arbetsplatssystem, webbplattform, e-tjänstplattform och gemensam integrationsplattform. Därtill finns lokala lösningar som används av en eller flera nämnder eller styrelser. När lokala digitala lösningar går mot slutet av sin livscykel ska staden i första hand undersöka om de kan ersättas med en gemensam digital lösning.

För att få mer detaljer och beskrivningar av den gemensamma it-infrastruktur och plattformar kontakta stadsledningskontoret, avdelningen för it och digitalisering på: Funktion.it@stockholm.se.

Eventuell ansökan om undantag från denna tillämpningsanvisning hanteras av avdelningen för it och digitalisering i samråd med berörd/berörda objektsägare och beslut fattas i enlighet med stadsledningskontorets delegationsordning.

2 Ansvar

Kommunstyrelsen ansvarar för förvaltning och utveckling av den centrala it-infrastrukturen och plattformarna. Kommunstyrelsen ansvarar även för att upprätta och förvalta de centrala avtal som krävs för att leverera dessa tjänster till stadens nämnder och styrelser. Avtal finns med externa parter samt med de av staden ägda bolagen Stokab och S:t Erik kommunikation AB.

Stadens nämnder och styrelser ansvarar för att beställa de tjänster som de har behov av genom att lägga beställningar i de avtal som Kommunstyrelsen tillhandahåller.

Kommunstyrelsen ansvarar för att etablera och underhålla rutiner för beställning, behovsinsamling, ändringshantering och undantagshantering rörande den centrala infrastrukturen och plattformarna. Stadens nämnder och styrelser ansvara för att följa de rutiner Kommunstyrelsen fastlagt.

3 Central it-infrastruktur och plattformar

3.1 Digital arbetsplats

Den digitala arbetsplatsen är de tjänster, programvaror och den hårdvara som användare behöver inom ramen för tjänsteutövandet och för att få åtkomst till stadens olika verksamhetssystem och andra informationskällor inom och utanför staden. Arbetsplatsen består av stationära och mobila digitala enheter[1], programvaror, kringutrustning samt de gemensamma plattformar som behövs för drift och support av de digitala enheterna. Plattformarna innehåller tjänster för hantering och övervakning av digitala enheter samt drift och support av gemensamma tjänster såsom självservice, e-post, samarbetsytor, lagring, utskrift och videokonferens.

Digital arbetsplats är gemensam för staden och får inte ersättas med lokala lösningar.

3.2 Servicedesk

Stadens servicedeskar ska vara den första linjens kontakt för användarfrågor för stadens hela it-miljö. Stadens servicedeskar har, utöver att hantera frågor direkt, ansvar för att förmedla ärenden till andra och tredje linjens support vilket tillhandahålls av olika leverantörer kopplat till de tjänster de levererar.

Servicedesk är gemensam för staden och får de inte ersättas med lokala lösningar.

3.3 Applikationsplattformar

Stadens applikationsplattformar är värdmiljöer som används för drift av stadens applikationer, system och tjänster. I applikationsplattformarna finns tjänster för serverdrift, databaser, databashotell, e-tjänster, virtualiseringsplattformar, webbhotell och CRM-lösningar.

Applikationsplattformar är gemensam för staden och får inte ersättas med lokala lösningar.

[1] Exempelvis mobiler, surfplattor och datorer med tillhörande operativsystem

3.4 Integrationsplattformar

Stadens integrationsplattformar sammankopplar och underlättar etablering och förvaltning av integrationer mellan olika applikationer, system, IoT-komponenter och tjänster inom och utanför staden. Integrationer mellan system består av olika former av automatiserade funktionella och fysiska informationsutbyten. Staden har gemensamma metoder för att automatisera processer, ansluta applikationer, ansluta sensorer och hantera strömmande data.

Integrationsplattformar är gemensamma för staden och får inte ersättas med lokala lösningar. Området IoT är under uppbyggnad, samråd med stadsledningskontoret ska ske innan införande av IoT-tillämpningar.

3.5 Identitets- och åtkomsthantering

Staden har gemensamma tekniska lösningar för identitets- och åtkomsthantering, säkra meddelanden och för elektronisk underskrift.

För identifiering[2] tillhandahåller staden stadsövergripande tekniska lösningar och autentiseringsmetoder. Information om alla användaridentiteter är samlad i en katalogstruktur godkänd av stadsledningskontoret.

Behörighetshantering[3] hanteras i de flesta fall i respektive system eller tjänst. Val av tekniska lösningar för behörighetshantering ska ske i samråd i med stadsledningskontoret.

Stadens har en gemensam tjänst för att skicka säkra meddelanden med känslig information, både internt och externt, på ett säkert och lagenligt sätt.

Staden har en gemensam tjänst för elektronisk underskrift. En elektronisk underskrift är den elektroniska motsvarigheten till underskrift för hand på ett papper.

Identitets- och åtkomsthantering, säkra meddelanden och elektronisk underskrift är gemensamma tjänster för staden och får inte ersättas med lokala lösningar. Ansvaret för behörighetshantering ligger på respektive objektsägare i samråd med stadsledningskontoret.

---

[2] Identifiering är att säkerställa att någon är den som den uppger sig vara.
[3] Behörighetshantering (auktorisering) är att säkerställa att en identifierad användare har rätt behörigheter.

3.6 Grundläggande infrastruktur

Staden har ett gemensamt datakommunikationsnätverk. Nätverket består av fysiska och logiska nätverk, accesslösningar och ett antal olika tekniker för att möjliggöra säker digital kommunikation. Stadens nätverk och accesslösningar används för att få tillgång till internet samt övriga interna och externa digitala tjänster som verksamheten nyttjar.

I grundläggande infrastruktur ingår säker anslutning till stadens nätverk, internet och omvärldsuppkoppling till exempelvis stadens upphandlade tjänsteleverantörer. Det ingår även tjänster för säker åtkomst, grundläggande IP-tjänster[4], grundläggande it-säkerhetstjänster[5] och installation och anslutning av lokal nätverksutrustning.

Grundläggande infrastruktur är gemensam för staden och får inte ersättas med lokala lösningar.

3.7 Stockholm webb

I stort sett alla stadens publika webbplatser, undantaget bolagssfären där lokala plattformar nyttjas, ingår i Stockholm webb. På stadens webbplatser finns information till invånare, näringsliv och andra intressenter och via webbarna nås merparten av stadens digitala service/e-tjänster. Grundläggande för webbplatserna är att de utformas utifrån kunskaper om användarnas behov och för att stödja verksamhetseffektivitet. I objektet ingår toppdomänen .stockholm, multisajten .stockholm, stadsövergripande intranät, miniwebbar, verksamhetswebbar, kartmanér och server för nyhetsbrev.

Stockholm webb är gemensam för staden och får inte ersättas med lokala lösningar

3.8 Datalager

Objektet Beslutsstöd är stadens centrala stöd för business intelligence. Syftet är att stödja stadens verksamheter med verksamhetsdata för rapporter och analyser. Beslutstöd ger stadens verksamheter stöd i att planera, analysera, följa upp och utveckla sin verksamhet. I Beslutsstöd ingår datalager för lagring av verksamhetsdata, semantiska lager för att översätta data till verksamhetsbegrepp, en rapport- och analysplattform samt en portal där rapporter publiceras.

Stadens centrala stöd för business intelligence är gemensamt för staden men kan vid behov kompletteras med lokala lösningar. Om behov finns av sådana lösningar ska samråd ske med stadsledningskontoret.

---

[4] Exempelvis namnuppslag och IP-planadministration (DHCP, DNS, IPAM).
[5] Exempelvis webbfilter, brandväggar, DDoS-skydd, sårbarhetsanalys/nätverksscanning.

3.9 Geodataplattform

Staden har en central geodataplattform för behandling av geodata. SGIS (Stockholms stads geografiska informationssystem) innehåller system för att lagra, bearbeta och presentera geodata. Genom kart- och webbklinter får användare tillgång till kartinformation och annan geografisk information. Staden har även en metadataportal som kan användas för att tillgängliggöra stadens geodata, och göra den sökbar. Det finns även en konverteringsportal för olika geodataformat.

Stadens centrala geodataplattform är gemensam för staden men kan vid behov kompletteras med lokala lösningar. Om behov finns av sådana lösningar ska samråd ske med stadsledningskontoret.

Instruktion

Komplett ifylld bilaga - Kravspecifikation ska bifogas anbudet.

De krav som leverantören uppfyller ska ingå i anbudspriset. Kravspecifikationen är indelad i flikar enligt följande:
1. Funktionella krav
2. Icke-funktionella krav
3. Informationssäkerhetskrav

Anbudsgivaren ska fylla i samtliga gula fält (kolumn E). Det är av största vikt att anbudsgivaren lämnar svar om kravet uppfylls eller inte uppfylls i samtliga gulmarkerade fält. Uteblivet svar tolkas som att kravet inte uppfylls. Om anbudsgivare vill förtydliga/beskriva hur kravet uppfylls eller annat av betydelse kopplat till kravet kan kolumn F användas.

Förklaring till kolumnerna i flikarna:

Kolumn A: ID	En unik identifierare för kravet	
Kolumn B: Kravområde		
Kolumn C: Krav		
Kolumn D: Ska / Bör	Ska – Obligatoriskt krav som anbudet måste inkludera. Alla kraven i flik "Informationssäkerhetskrav" är obligatoriska. Bör – Kravet är inte obligatoriskt, men ger mervärdespoäng i utvärderingen	
Kolumn E: Uppfylls kravet?	Svar från anbudsgivaren om anbudet inkluderar en lösning för det uttryckta kravet Ja = inkluderas i anbudet Nej = inkluderas inte i anbudet	
Kolumn F: Mervärde börkrav	Procent av max poäng för de funktionella börkraven, som tilldelas anbudsgivare som uppfyller Bör-krav, utgör underlag för utvärdering	Svar från anbudsgivaren om anbudet inkluderar en lösning för det uttryckta kravet Ja = inkluderas i avtalet Nej = inkluderas inte i avtalet

Funktionella krav

				Anbudsgivaren besvarar dessa kolumner		
ID	**Delområde**	**Krav**	**Ska/Bör**	**Uppfylls kravet? Ja/Nej**	**Anbudsgivarens kommentar**	**Mervärde börkrav**
1.1	Övergripande	Som ställföreträdare vill jag få stöd i vilka uppgifter som ska fyllas i utifrån uppdragets omfattning (Fullt godmanskap, Fullt förvaltarskap, Förvalta egendom, Bevaka rätt, Sörja för person) för att underlätta arbetet	Ska			
1.2	Övergripande	Som systemadministratör vill jag kunna ställa in vilka fält som ska visas utifrån uppdragets omfattning för att underlätta arbetet	Bör			7%
1.3	Övergripande	Som användare vill jag kunna ha flera flikar för olika huvudmän uppe samtidigt för att kunna arbeta parallellt med olika vyer i systemet	Ska			
1.4	Övergripande	Som ställföreträdare vill jag att det i alla vyer är tydligt vilken huvudman informationen avser	Ska			
1.5	Övergripande	Som användare vill jag att det tydligt framgår vilka uppgifter som är obligatoriska att fylla i för att underlätta dokumentationen	Ska			
1.6	Övergripande	Som systemadministratör vill jag kunna ställa in vilka uppgifter som ska vara obligatoriska att fylla i för att underlätta dokumentationen	Bör			7%
1.7	Övergripande	Som användare vill jag kunna söka, sortera och filtrera information i olika vyer och i journal/dagbok	Ska			
1.8	Övergripande	Som användare vill jag kunna se hjälptexter i systemet för att underlätta mitt arbete.	Ska			
1.9	Övergripande	Som systemadministratör vill jag kunna redigera hjälptexter för att uppdatera informationen	Bör			14%
1.10	Övergripande	Som systemadministratör vill jag kunna ställa in generella påminnelser för att ge stöd i arbetet	Ska			
1.11	Övergripande	Som användare vill jag kunna ställa in egna påminnelser för att få stöd i arbetet	Ska			
1.12	Övergripande	Som användare vill jag kunna välja om påminnelse ska tas bort helt eller senareläggas	Ska			
1.13	Övergripande	Som ställföreträdare vill jag kunna sätta upp en egen planering med arbetsuppgifter och mål kopplat till ett ärende för att underlätta mitt arbete	Ska			
1.14	Övergripande	Som ställföreträdare vill jag kunna följa upp min egen planering med arbetsuppgifter och mål för att underlätta mitt arbete	Ska			
1.15	Övergripande	Som ställföreträdare vill jag kunna få fram länkar till mallar för att säkerställa att rätt version används (exempelvis olika ansökningsblanketter från skatteverket och socialtjänsten)	Ska			
1.16	Övergripande	Som ställföreträdare vill jag att systemet automatiskt fyller i vissa uppgifter i formulär och mallar för att få stöd i arbetet	Ska			
1.17	Övergripande	Som systemadministratör vill jag kunna skapa mallar för att underlätta arbetet (exempelvis brevmallar, överklagan, yttrande)	Ska			
1.18	Övergripande	Som användare vill jag kunna använda mallar och justera text i mallar för att få stöd i arbetet	Ska			

1.19	Övergripande	Som ställföreträdare vill jag kunna kategorisera och spara dokument i systemet (minst i följande format: PDF, Word, Excel, JPEG) för att möjliggöra digital hantering av ärenden	Ska			
1.20	Övergripande	Som ställföreträdare vill jag kunna importera inskannade handlingar för att spara handlingarna digitalt i systemet	Ska			
1.21	Övergripande	Som användare vill jag kunna bifoga dokument genom "drag-and-drop" funktion	Bör			16%
1.22	Övergripande	Som användare vill jag kunna skicka meddelande till annan användare i systemet för att dela viktig information (exempelvis chatt-funktion eller gemensamma arbetsanteckningar)	Bör			1%
1.23	Övergripande	Som systemadministratör vill jag kunna skicka notiser till en eller alla användare för att underlätta kommunikationen	Bör			1%
1.24	Övergripande	Som användare vill jag kunna skicka och ta emot sms i systemet för att underlätta kommunikation med huvudmän och kontaktpersoner	Bör			1%
1.25	Övergripande	Som användare vill jag kunna kategorisera och spara e-mail i systemet för att få en samlad bild av ärendet	Ska			
1.26	Övergripande	Som användare vill jag kunna skriva ut vyer och sammanställningar för att enkelt få ut information på papper	Ska			
1.27	Övergripande	Som användare vill jag kunna gallra information och ärenden i systemet utifrån förbestämda kriterier för att underlätta gallring	Ska			
1.28	Fördela och följa upp ärenden	Som systemadministratör vill jag kunna lägga till och ta bort nya användare för att säkerställa korrekt behörighetshantering	Ska			
1.29	Fördela och följa upp ärenden	Som systemadministratör vill jag kunna tilldela, ta bort och justera behörigheter för att säkerställa korrekt behörighetshantering	Ska			
1.30	Fördela och följa upp ärenden	Som systemadministratör vill jag kunna tilldela användare olika typer av behörighet till specifika ärenden, exempelvis tittbehörighet, begränsad behörighet och fullständig behörighet.	Ska			
1.31	Fördela och följa upp ärenden	Som systemadministratör vill jag kunna tilldela flera användare delat uppdrag i ärenden kopplat till personligt förordnande	Ska			
1.32	Fördela och följa upp ärenden	Som samordnare vill jag kunna fördela inkomna ärenden till ställföreträdare för att säkerställa en jämn arbetsfördelning	Ska			
1.33	Fördela och följa upp ärenden	Som ställföreträdare vill jag kunna skapa granskningsdokument med ekonomisk redovisning för föregående månad för att möjliggöra interngranskning	Ska			
1.34	Fördela och följa upp ärenden	Som ställföreträdare vill jag kunna ge interngranskare tillgång till granskningsdokument med underlag för att möjliggöra interngranskning	Ska			
1.35	Fördela och följa upp ärenden	Som interngranskare vill jag kunna granska ställföreträdares ekonomiska redovisning med underlag för att säkerställa korrekt hantering av ärenden	Ska			
1.36	Fördela och följa upp ärenden	Som interngranskare vill jag kunna göra noteringar kopplat till granskningsdokument med underlag	Ska			
1.37	Fördela och följa upp ärenden	Som interngranskare vill jag kunna klarmarkera en interngranskning för att underlätta uppföljning	Ska			
1.38	Fördela och följa upp ärenden	Som interngranskare vill jag kunna markera och kommentera om en klarmarkerad granskning gjordes med eller utan anmärkning för att underlätta uppföljning	Ska			

1.39	Fördela och följa upp ärenden	Som interngranskare vill jag att granskningsdokument med underlag för interngranskning raderas när ärendet klarmarkerats utan anmärkning	Bör			4%
1.40	Fördela och följa upp ärenden	Som interngranskare vill jag att det skapas en lista med ärenden för interngranskning för att kunna följa upp vilka ärenden som ska granskas och vilka ärenden som har granskats, med notis om anmärkning och eventuell kommentar till anmärkning	Ska			
1.41	Fördela och följa upp ärenden	Som interngranskare vill jag att systemet ska kunna välja ut ett slumpmässigt urval ärenden för granskning utifrån förbestämda parametrar för att underlätta interngranskning	Bör			7%
1.42	Fördela och följa upp ärenden	Som användare vill jag enkelt kunna få fram avidentifierad statistik för att analysera verksamhetens resultat och utveckling	Ska			
1.43	Fördela och följa upp ärenden	Som användare vill jag kunna få fram statistik över hur lång tid uppdragen är i respektive status för att följa upp arbetsflödet	Bör			17%
1.44	Fördela och följa upp ärenden	Som användare vill jag kunna exportera statistiken till Excel för att möjliggöra vidare bearbetning	Ska			
1.45	Fördela och följa upp ärenden	Som användare vill jag kunna avsluta uppdrag och ärenden	Ska			
1.46	Fördela och följa upp ärenden	Som användare vill jag att avslutade ärenden ska sparas tills informationen ska rensas utifrån uppsatta regler	Ska			
1.47	Hantera ärenden	Som ställföreträdare vill jag ha en startsida med information om mina pågående ärenden, påminnelser och kommande arbetsuppgifter för att få en tydlig övergripande bild över mitt arbete	Ska			
1.48	Hantera ärenden	Som ställföreträdare vill jag ha en checklista med uppgifter som ska kontrolleras vid uppstart av varje nytt ärende	Ska			
1.49	Hantera ärenden	Som ställföreträdare vill jag kunna ändra status för ett ärende för att kunna följa ärendet	Ska			
1.50	Hantera ärenden	Som ställföreträdare vill jag ha en vy för varje huvudman med namn, personnummer, kontaktuppgifter, information om kontaktpersoner och uppdrag	Ska			
1.51	Hantera ärenden	Som ställföreträdare vill jag ha en vy för varje ärende med samlad information för att få en översiktlig bild av ärendet	Ska			
1.52	Hantera ärenden	Som användare vill jag kunna lägga upp en ny huvudman	Ska			
1.53	Hantera ärenden	Som ställföreträdare vill jag kunna registrera uppgifter om huvudman för att kunna utföra mitt uppdrag	Ska			
1.54	Hantera ärenden	Som ställföreträdare vill jag att systemet hämtar och hanterar uppgifter om huvudmän från folkbokföringsregistret för att ha tillgång till aktuella persondata	Ska			
1.55	Hantera ärenden	Som ställföreträdare vill jag kunna registrera persondata om huvudmän manuellt för att komplettera med uppgifter som inte finns med i folkbokföringsregistret.	Ska			
1.56	Hantera ärenden	Som ställföreträdare vill jag få en notis när uppgifter om huvudman ändras i folkbokföringsregistret för att få information om förändringen	Ska			
1.57	Hantera ärenden	Som ställföreträdare vill jag att systemet uppdaterar en huvudmans persondata när förändring skett i folkbokföringsregistret och att de gamla uppgifterna sparas i ärendet.	Ska			
1.58	Hantera ärenden	Som användare vill jag kunna markera personer med skyddade personuppgifter för att säkerställa korrekt hantering av information	Ska			

1.59	Hantera ärenden	Som användare vill jag kunna markera personer med riskbeteende för att underlätta arbetet	Ska			
1.60	Hantera ärenden	Som ställföreträdare vill jag kunna notera händelser i en journal/dagbok för att få en samlad bild av ärendet	Ska			
1.61	Hantera ärenden	Som systemadministratör vill jag kunna ställa in att vissa uppgifter automatiskt sparas i journal/dagbok för att underlätta arbetet	Ska			
1.62	Hantera ärenden	Som ställföreträdare vill jag kunna justera sparade uppgifter i journal/dagbok för att kunna komplettera eller rätta fel	Ska			
1.63	Hantera ärenden	Som ställföreträdare vill jag kunna få en automatisk sammanställning av data utifrån förbestämd mall för att redogöra för utfört uppdrag	Ska			
1.64	Hantera ärenden	Som ställföreträdare vill jag kunna registrera information om arvoden för att få underlag till utbetalning av arvoden	Ska			
1.65	Hantera ekonomi	Som ställföreträdare vill jag kunna hantera bokföring för huvudman för att underlätta arbetet	Ska			
1.66	Hantera ekonomi	Som ställföreträdare vill jag kunna göra en budget kopplat till huvudman för att hantera ekonomin	Ska			
1.67	Hantera ekonomi	Som ställföreträdare vill jag kunna importera transaktionsdata direkt från utvalda banker för att säkerställa en korrekt redovisning i systemet	Bör			25%
1.68	Hantera ekonomi	Som ställföreträdare vill jag kunna importera transaktionsdata via fil från bank för att säkerställa en korrekt redovisning i systemet	Ska			
1.69	Hantera ekonomi	Som ställföreträdare vill jag kunna lägga in kostnader/transaktioner manuellt för att säkerställa en korrekt redovisning i systemet	Ska			
1.70	Hantera ekonomi	Som ställföreträdare vill jag kunna kategorisera vissa typer av kostnader/transaktioner manuellt för att kunna få ut en sammanställning av alla kostnader inom kategorin	Ska			
1.71	Hantera ekonomi	Som ställföreträdare vill jag kunna skriva vad varje kostnad avser för att möjliggöra korrekt redovisning	Ska			
1.72	Hantera ekonomi	Som ställföreträdare vill jag kunna bifoga digitalt underlag till alla transaktioner för att möjliggöra digital hantering	Ska			
1.73	Hantera ekonomi	Som ställföreträdare vill jag att årsräkning summeras utifrån löpande räkenskaper för att underlätta arbetet (Tillgångar 1/1 + Inkomster; Utgifter + Tillgångar 31/12)	Ska			
1.74	Hantera ekonomi	Som ställföreträdare vill jag att systemet kontrollräknar summering och varnar om summeringen ej stämmer (Tillgångar 1/1 + Inkomster = Utgifter + Tillgångar 31/12)	Ska			
1.75	Hantera ekonomi	Som ställföreträdare vill jag kunna få en översiktlig sammanställning av bokföringen i siffror utifrån valda parametrar	Ska			
1.76	Hantera ekonomi	Som ställföreträdare vill jag kunna få en översiktlig sammanställning av bokföringen i grafisk form för att enkelt få en överblick över ekonomin utifrån valda parametrar	Ska			
1.77	Hantera ekonomi	Som ställföreträdare vill jag kunna skriva ut en sammanställning av ekonomin för att delge huvudman information som är enkel att förstå	Ska			
1.78	Hantera ekonomi	Som ställföreträdare vill jag kunna få en automatisk sammanställning av data utifrån förbestämd mall för att redovisa årsräkning och sluträkning för huvudman	Ska			

Icke-funktionella krav

				Anbudsgivaren besvarar dessa kolumner	
ID	**Delområde**	**Krav**	**Ska/Bör**	**Uppfylls kravet? Ja/Nej**	**Anbudsgivarens kommentar**
2.1	Design och arkitektur	Systemet ska vara helt integrerat, alla installerade systemmoduler fungerar smidigt och korrekt tillsammans och skapar nödvändiga transaktioner i alla berörda moduler i realtid.	Ska		
2.2	Design och arkitektur	Systemet ska i full utsträckning vara ett fleranvändarsystem	Ska		
2.3	Design och arkitektur	Systemstödet och implementeringen i sin helhet ska ske i enlighet med Stadens riktlinjer för informationssäkerhet och genomförd informationsklassning, se bilaga Riktlinje för Informationssäkerhet	Ska		
2.4	Design och arkitektur	Systemets gränssnitt och rapporter ska genomgående vara på svenska	Ska		
2.5	Design och arkitektur	Systemet ska följa tillgänglighet enligt WCAG 2.1 AA	Ska		
2.6	Design och arkitektur	Systemets sökgränssnitt ska tillåta (och exekverar sökning) att uppgifter skrivs in på olika sätt.	Ska		
2.7	Design och arkitektur	Systemets användargränssnitt ska följa normal fönsterhantering (t.ex. flera fönster med olika eller lika funktioner kan öppnas samtidigt), enligt MS Windows eller webbformatstandard.	Ska		
2.8	Datakommunikation	Systemet ska använda stadens befintliga WiFi-miljö som består av WiFi accesspunkter i infrastructure mode	Ska		
2.9	Prestanda	Systemet ska kunna hantera minst 30 samtidiga användare med bibehållen prestanda.	Ska		
2.10	Prestanda	Konfigurering av systemlösningen ska genomföras på ett sådant sätt att systemet ska kunna hantera växande volymer av data med bibehållen prestanda under hela avtalstiden.	Ska		
2.11	Tillgänglighet	Systemet ska vara tillgängligt 98 % på månadsbasis	Ska		
2.12	Tillgänglighet	Tillgängligheten för systemet skall under årets samtliga helgfria arbetsdagar vara kl. 07.00–18.00	Ska		
2.13	Drift	Systemet ska kunna driftas av oberoende extern part och systemdrift skall ej vara knuten till en part	Ska		
2.14	Drift	Drift av infrastruktur ska kunna frikopplas från applikationsförvaltning	Ska		
2.15	Underhåll och support	Leverantörens stödorganisation ska ha antagit en standardiserad process för att hantera incidenter, problem och förändringar.	Ska		
2.16	Underhåll och support	Leverantörens stödfunktion ska logga alla inkommande incidenter och erbjuder uppföljning och förbättringsförslag för alla upprepade incidenter som rapporterats av Arbetsmarknadsförvaltningen.	Ska		
2.17	Underhåll och support	Verksamheten ska ha möjlighet att påverka servicefönstret för patchningar och liknande tekniska aktiviteter för att dagliga aktiviteter ska påverkas minimalt.	Ska		
2.18	Underhåll och support	Svensktalande support (ifall leverantören ska ha direktkontakt med Staden)	Ska		
2.19	Behörighet	Systemet ska ha stöd för Single-Sign-On (SSO), gentemot Stadens interna katalogtjänst (AD).	Ska		
2.20	Behörighet	Systemet ska innehålla funktion för behörighetskontroll.	Ska		
2.21	Behörighet	Systemstödet ska ha funktionalitet för att styra och begränsa användares åtkomst till funktionalitet och information i systemstödet baserat på behörighet och roll.	Ska		
2.22	Behörighet	Systemstödet ska ha funktionalitet för att styra användares rättigheter till att läsa, skriva och redigera baserat på behörighet och roll.	Ska		

2.23	Spårbarhet	Ändringar ska loggas. Det ska vara lätt att spåra vem som gjorde vilken förändring och när.	Ska		
2.24	Spårbarhet	Systemet ska innehålla verifieringskedjor / historik på importerade externa filer, som ger information om vilka filer som har importerats, när och av vem, inklusive eventuella meddelanden om systemfel.	Ska		
2.25	Spårbarhet	Systemstödet ska innehålla funktion för att härleda en användares identitet i behörighetskontrollsystemet.	Ska		
2.26	Uppdateringar och säkerhet	Systemet ska uppdateras med nya säkerhetsuppdateringar vid behov	Ska		
2.27	Uppdateringar och säkerhet	Systemet ska under hela livscykeln upprätthålla en säkerhetsnivå som minst motsvarar kravställningarna från klassningsresultatet samt stadens anvisningar	Ska		
2.28	Uppdateringar och säkerhet	Leverantören ska ha etablerade rutiner och processer för att löpande och under hela produktens livscykel säkerställa att säkerhetskraven efterlevs	Ska		
2.29	Uppdateringar och säkerhet	Lösningen ska ha säker rollbaserad (valserad) åtkomst till gränssnitt och funktioner	Ska		
2.30	Uppdateringar och säkerhet	Nya versioner av systemet, dess uppgraderingar och patchar ska inkluderas i avtalet utan extra kostnad för beställaren.	Ska		
2.31	Säkerhetskopiering och backup	Det bör vara möjligt att göra en fullständig säkerhetskopia av systemet inklusive systemfunktionalitet och databaser under normal systemdrift.	Bör		
2.32	Säkerhetskopiering och backup	Systemet bör innehålla funktioner för att garantera enhetlighet i både backup samt i systemet (funktionalitet och databaser) när en säkerhetskopiering utförs under normal drift.	Bör		
2.33	Säkerhetskopiering och backup	Under en säkerhetskopiering/återställning i systemet ska en fullständig spårbarhet (verifieringskedja) av transaktioner i systemet garanteras.	Ska		
2.34	Utveckling och implementering	Leverantören ska testa samtliga leveranser i separat testmiljö innan de införs i driftmiljö (produktion). Testdata ska skyddas, kontrolleras och får inte innehålla information som är känslig eller omfattas av sekretess eller på annat sätt strider mot dataskyddsförordningen.	Ska		
2.35	Dokumentation	Leverantören ska ansvara för att det finns en samlad och uppdaterad teknisk dokumentation, som beskriver alla ingående delar i systemet, och som görs tillgänglig för Staden vid behov. Den tekniska dokumentationen ska uppdateras löpande under hela avtalsperioden. Dokumentationen ska vara skriven på svenska och innehålla åtminstone följande delar: - En systemöversikt - Systemets databaser och tabeller - Driftsinstruktioner inklusive backuprutiner - Återstartsrutiner och andra instruktioner som krävs för att erhålla säker drift med avtalad tillgänglighet och svarstider för Stadens installation - Beroenden av tredjepartskomponenter	Ska		
2.36	Informationsutbyte med kringliggande system	Integrationer ska ske genom stadens Integrationsplattformar oavsett var systemet driftas - moln, on-prem etc enligt Stadens Kvalitetsprogram och dokumentet "Tillämpningsanvisning för central it-infrastruktur och plattformar" kapitel 3.4. se Bilaga - Tillämpningsanvisning för central it-infrastruktur och plattformar	Ska		

2.37	Informationsutbyte med kringliggande system	Lösningen ska stödja import av inskannade dokument så att de kan bearbetas i systemet.	Ska		
2.38	Informationsutbyte med kringliggande system	Systemet ska ha funktionalitet som säkerställer att importerad information är korrekt, dvs att data är i rätt format och att uppgifterna inte har manipulerats under importen.	Ska		
2.39	Informationsutbyte med kringliggande system	Systemet ska kunna importera/exportera information från/till Excel.	Ska		
2.40	Informationsutbyte med kringliggande system	Systemet ska tillhandahålla öppna API:er och via dessa möjliggöra integrationer för att dela information med ÖFF:s verksamhetssystem eller e-tjänst via filformat JSON vid överföring.	Ska		
2.41	Användarbarhet	Fält i systemets användargränssnitt som är låsta för redigering ska avvika utseendemässigt/grafiskt från fält som är möjliga att redigera.	Ska		
2.42	Användarbarhet	Det ska gå att kopiera värden från systemets användargränssnitt för inklistring i kontorsprogramvara utan vidare formatering.	Ska		
2.43	Gallring	Teknisk funktion för gallring ska finnas i IT-stödet.	Ska		
2.44	Gallring	Gallring ska kunna utföras i IT-stödet i enlighet med de gallringsfrister som anges i gallringsbeslut.	Ska		
2.45	Gallring	Resultat av begärd gallring ska kunna kontrolleras innan den utförs, för att undvika felaktig gallring.	Ska		
2.46	Gallring	Gallrad information ska inte kunna återskapas.	Ska		
2.47	Gallring	Det ska säkerställas att handlingar som ska gallras har ett format som möjliggör att de kan öppnas och läsas ända fram till att gallringsfristen har löpt ut.	Ska		
2.48	Gallring	Gallringsrapport/-logg ska kunna skapas i IT-stödet. Uppgifterna ska minst bestå av: tidpunkt för gallring, vem som utfört gallringen och vad som gallrats.	Ska		
2.49	Migrering	Information (t.ex. filer och metadata) ska kunna migreras till en annan databärare.	Ska		
2.50	Migrering	Vid migrering ska informationens struktur och samband kunna upprätthållas och sammanställningsmöjligheterna inte förvanskas eller försvinna.	Ska		
2.51	Migrering	Systemberoende länkar eller ID-begrepp ska vid migrering kunna översättas och kompletteras för att bibehålla informationens kontext.	Ska		

Informationssäkerhetskrav

				Anbudsgivaren besvarar dessa kolumner	
ID	**ISO kravområde**	**Krav** KLASSA upphandlingskrav (säkerhetsnivå 3 - 3 - 3)	**Ska/Bör**	**Uppfylls kravet? Ja/Nej**	**Anbudsgivarens kommentar**
3.1	A.6.2.2 Distansarbete	Leverantören ska ha dokumenterade rutiner för distansarbete. Informationsbehandlingen ska vara lika säker på distans som den är vid behandling på leverantörens arbetsplats.	Ska		
3.2	A.7.1.1 Bakgrundskontroll	Leverantören ska ha processer och rutiner på plats för relevant bakgrundskontroll av personal.	Ska		
3.3	A.7.1.2 Anställningsvillkor	Leverantören ska ha avtal om tystnadsplikt med sina anställda. Tystnadsplikten ska omfatta information om leverantörens kunder. Via avtal ska leverantören även säkerställa tystnadsplikt för underleverantörer. Detta krävs dock inte om dessa redan omfattas av en straffsanktionerad tystnadsplikt som följer av lag.	Ska		
3.4	A.7.2.2 Medvetenhet, utbildning och fortbildning vad gäller informationssäkerhet	Leverantören ska för sin personal varje halvår genomföra utbildningar för ökad medvetenhet kring informationssäkerhet samt hålla sig uppdaterad kring beställarens policys, regler och rutiner.	Ska		
3.5	A.7.2.3 Disciplinär process	Leverantören ska ha en tydlig och disciplinär process med åtgärder för anställda som har brutit mot informationssäkerhetsregler.	Ska		
3.6	A.7.3.1 Avslut eller ändring av anställds ansvar	Leverantören ska till personalen ha kommunicerat de ansvar och skyldigheter som förblir gällande efter ändring eller avslut av anställning. Personalen ska ha skrivit under en ansvarsförbindelse avseende detta.	Ska		
3.7	A.8.1.3 Tillåten användning av tillgångar	Leverantören ska ha dokumenterade regler, rutiner och roller som beskriver tillåten användning av de resurser (t.ex. arbetsdatorer, bärbara datorer eller mobila enheter). som ingår i leveransen. Leverantören ska årligen kontrollera att de efterlevs.	Ska		
3.8	A.8.1.4 Återlämnande av tillgångar	Leverantören ska ha rutiner och funktioner för att återlämna beställarens fysiska och elektroniska tillgångar då anställning, uppdrag eller avtal upphör. Leverantören ska på begäran kunna uppvisa underlag på att så skett.	Ska		
3.9	A.8.2.1 Klassning av information	Leverantören ska följa beställarens rutiner och processer för informationsklassning samt tillämpa relevanta säkerhetsåtgärder.	Ska		
3.10	A.8.2.3 Hantering av tillgångar	Beställarens krav på informationshanteringen ska efterföljas i relation till beställarens informationsklassning. Om sådana krav inte ställts ska leverantören utan anmodan kunna uppvisa de rutiner som gäller hos leverantören för hantering av beställarens tillgångar.	Ska		
3.11	A.9.2.1 Registrering och avregistrering av användare	Leverantören ska ha en formell och dokumenteras process för hur användaridentiteter hanteras (registrering och avregistrering). Leverantören ska säkerställa att användaridentiteterna hos leverantör och beställare är personliga och unika över tid. Se tillitsramverket (ELN0700) tillitsnivå 3 (LoA3) för detaljer.	Ska		

3.12	A.9.2.2 Tilldelning av användaråtkomst	Leverantören ska följa en överenskommelse för användaråtkomst till beställarens system, tjänster och information. Endast behöriga och enligt överenskommelsen godkända individer ska inneha åtkomst. Hanteringen ska vara spårbar och redovisas för beställaren enligt överenskommelse, minst årligen.	Ska		
3.13	A.9.2.3 Hantering av privilegierade åtkomsträttigheter	Leverantören ska använda särskilda personliga användaridentiteter för systemadministration. Dessa konton ska vara spårbara och lätta att skilja från vanliga användare. Leverantören ska ha särskilda säkerhetsåtgärder kopplade till systemadministration. (Exempelvis tidsbegränsade behörigheter eller striktare autentisering)	Ska		
3.14	A.9.2.4 Hantering av användares konfidentiella autentiseringsinformation	Leverantören ska på ett säkert sätt distribuera, lagra och återställa autentiseringsinformation (exempelvis lösenord) utan att det kan röjas till obehöriga. Autentiseringsinformation får ej lagras i klartext (gäller även systemkonton i källkod). Se vägledning för tillitsnivå 3 (LoA3) för detaljer.	Ska		
3.15	A.9.2.5 Granskning av användares åtkomsträttigheter	Leverantören ska granska sina användares åtkomsträttigheter halvårsvis, Obehöriga eller användare som inte längre behöver åtkomst ska tas bort. Förändringar av åtkomsträttigheter ska dokumenteras av Leverantören och ska vid begäran tilldelas till beställaren	Ska		
3.16	A.9.2.6 Borttagning eller justering av åtkomsträttigheter	Leverantören ska ha en rutin för att permanent ta bort användaridentiteter från information, tjänster och system, vid avslutande av anställning, avtal eller uppdrag. Kontroll av efterlevnad ska ske årligen.	Ska		
3.17	A.9.3.1 Användning av konfidentiell autentiseringsinformation	Leverantören ska för sin personal ha fastställda regler för hur autentiseringsinformation ska skyddas och hanteras.	Ska		
3.18	A.9.4.1 Begränsning av åtkomst till information	Leverantören ska ha systemfunktioner för att begränsa åtkomst till information. Behörigheterna ska tilldelas enligt principen där minsta möjliga behörighet tilldelas utifrån en användares roll och arbetsuppgifter. Detta gäller även konton som används vid kommunikation mellan systemkomponenter samt priviligierade konton. Endast information eller tjänster som ska vara publika ska kunna nås i system utan godkänd autentisering.	Ska		
3.19	A.9.4.2 Säkra inloggningsrutiner	Leverantören ska tillse att autentiseringen till beställarens information, tjänster och system ska vara flerfaktorsbaserad i enlighet med kraven som följer av ELN0700. Endast utfärdare godkända av E-legitimationsnämnden (minst nivå 3) eller anslutna inom eIDAS (minst nivå substantiell) rekommenderas. Se vägledning för tillitsnivå 3 (LoA3) för detaljer.	Ska		
3.20	A.9.4.3 System för lösenordshantering	Leverantören ska tillse att information, tjänster och system har funktioner för att kunna kravställa autentiseringsinformation (pinkod, lösenord etc.) vad gäller komplexitet, längd och livslängd. Se vägledning för tillitsnivå 3 (LoA3) för detaljer.	Ska		
3.21	A.9.4.4 Användning av privilegierade verktygsprogram	Leverantören ska skydda och tillse att det finns spårbarhet i de verktyg som avses för underhåll och säkerhetskonfiguration för information, tjänster och system.	Ska		

3.22	A.9.4.5 Åtkomstkontroll till källkod för program	Leverantören ska tillse att källkod framtagen i egen utveckling skyddas från obehöriga förändringar. Källkod ska deponeras på ett sådant sätt att beställaren garanteras tillgång om leverantören inte uppfyller sina avtalade förpliktelser.	Ska		
3.23	A.10.1.1 Regler för användning av kryptografiska säkerhetsåtgärder	Leverantören ska ha rutiner för kryptering där val av algoritmer, protokoll och nyckellängder samt hantering av krypteringsnycklar framgår.	Ska		
3.24	A.11.1.1 Fysiska säkerhetsavgränsningar	Leverantören ska tillse att fysiska avgränsningar är definierade och tillämpade för skydd av områden med känslig eller kritisk information. Om det avser en datahall eller motsvarande ska leverantören tillse att den uppfyller minst skyddsnivå 3 ("datahall" enligt MSB "Vägledning för fysisk informationssäkerhet i it-utrymmen") eller likvärdigt.	Ska		
3.25	A.11.1.2 Fysiska tillträdesbegränsningar	Leverantören ska ha rutiner som säkerställer att endast behörig personal har fysisk åtkomst till områden med konfidentiell information, exempelvis en datahall.	Ska		
3.26	A. 12.1.1 Dokumenterade driftsrutiner	Leverantören ska dokumentera ansvar för driftsrutiner och göra de tillgängliga för användare som behöver dem.	Ska		
3.27	A.12.1.2 Ändringshantering	Leverantören ska ha rutiner för att planera, genomföra och dokumentera alla förändringar som påverkar leveransens säkerhet. Större förändringar ska följas upp, kontrolleras och redovisas minst årligen för beställaren.	Ska		
3.28	A.12.1.3 Kapacitetshantering	Leverantören ska ha funktioner, processer och rutiner för att övervaka och göra prognoser avseende framtida krav på systemprestanda.	Ska		
3.29	A.12.1.4 Separation av utvecklings-, test och driftmiljöer	Leverantören ska testa samtliga leveranser i separat testmiljö innan de införs i beställarens driftmiljö (produktion). Testdata ska skyddas, kontrolleras och får inte innehålla information som är känslig eller omfattas av sekretess.	Ska		
3.30	A.12.2.1 Säkerhetsåtgärder mot skadlig kod	Leverantören ska skydda mot skadlig kod. Det genom att ha säkerhetsåtgärder som inbegriper följande områden: förebygga, upptäcka, hantera och återställa Säkerhetsåtgärderna ska ses över minst årligen.	Ska		
3.31	A.12.3.1 Säkerhetskopiering av information	Leverantören ska ha rutiner och funktioner för säkerhetskopiering och återställande av information enligt överenskomna tillgänglighetskrav med beställaren. Säkerhetskopior ska skyddas på motsvarande sätt som originalinformationen. De ska förvaras på annan plats och på tillräckligt avstånd för att inte utsättas för eventuella skador vid katastrof på det ordinarie driftstället.	Ska		
3.32	A.12.4.1 Loggning av händelser	Leverantören ska tillse att information, tjänster och system har loggningsfunktioner för säkerhetsrelaterade händelser, minst för felaktiga inloggningar, förändring av behörigheter, otillåten anslutning samt överträdelser av behörigheter. Loggning ska ske i samråd med beställaren. Leverantören ska aktivt använda loggarna för att upptäcka och hantera incidenter. Beställaren ska kunna genomföra granskning av loggar vid behov.	Ska		
3.33	A.12.4.2 Skydd av logginformation	Leverantören ska skydda loggningsfunktioner och loggningsverktyg mot manipulation och obehörig åtkomst som även omfattar leverantörens personal.	Ska		

3.34	A.12.4.4 Synkronisering av tid	Leverantören ska tillse att information, tjänster och system, samt relaterad infrastruktur använder tidssynkronisering mot en och samma tidskälla(GPS eller svenska UTC (SP)).	Ska		
3.35	A.12.5.1 Installation av program på driftsystem	Leverantören ska verifiera och begränsa den mjukvara som får installeras på driftsystem.	Ska		
3.36	A.12.6.1 Hantering av tekniska sårbarheter	Leverantören ska bedriva ett kontinuerligt arbete för att identifiera sårbarheter och utan dröjsmål informera en utpekad funktion hos beställaren om de kan innebära ett hot för beställarens information, tjänster och system. Upptäckta sårbarheter ska åtgärdas omgående	Ska		
3.37	A.13.1.1 Säkerhetsåtgärder för nätverk	Leverantören ska säkerställa att all kommunikation till och från system, tjänster eller information ska vara skyddad mot obehörig åtkomst eller förvanskning. Det avser kommunikation mellan klient och server och mellan olika systemkomponenter. Skyddet ska uppdateras löpande utifrån kända sårbarheter.	Ska		
3.38	A.13.1.3 Separation av nätverk	Leverantören ska tillhandahålla en (logisk eller fysiskt) separerad kundmiljö inklusive behörighetskontrollsystem, loggar och lagring för varje kund.	Ska		
3.39	A.13.2.1 Regler och rutiner för informationsöverföring	Leverantören ska följa en överenskommelse med beställaren angående krav för informationsöverföring.	Ska		
3.40	A.14.1.1 Analys och specifikation av informationssäkerhetskrav	Leverantören ska ha fastlagda och dokumenterade principer och metoder för utveckling av säkra tjänster och system. Vid utveckling av webbapplikationer eller tillhandahållande av tjänster över publika nätverk ska OWASPs (www.owasp.org) rekommendationer följas	Ska		
3.41	A.14.1.2 Säkerställande av programtjänster på publika nätverk	Leverantören ska ha infört säkerhetsåtgärder som skyddar information i programtjänster på publika nätverk mot obehörig åtkomst och obehörig ändring. Vid utveckling av mobila appar ska OWASP Mobile App Security Checklist följ	Ska		
3.42	A.14.2.2 Rutiner för hantering av systemändringar	Leverantören ska ha riktlinjer för systemförändringar som avser informationssäkerhet inom sina utvecklingsprocesser. Vid större ändringar ska leverantören identifiera och hantera risker som säkerställer att säkerhetskraven i system eller tjänster är uppfyllda.	Ska		
3.43	A.14.2.3 Teknisk granskning av tillämpningar efter ändringar i driftsmiljö	Leverantören ska ha rutiner för att granska och testa tillgänglighet och säkerhet efter ändringar i verksamhetskritiska driftsplattformar.	Ska		
3.44	A.14.2.4 Restriktioner för ändringar av programpaket	Leverantören ska ha riktlinjer och instruktioner om beställaren avser att göra egna förändringar i programpaket.	Ska		
3.45	A.14.2.7 Outsourcad utveckling	Leverantören ska övervaka och styra systemutveckling som är utlagd till en underleverantör.	Ska		
3.46	A.15.1.1 Informationssäkerhetsregler för leverantörsrelationer	Leverantören ska följa beställarens rutiner och processer för åtkomst till organisationens tillgångar.	Ska		
3.47	A.16.1.1 Ansvar och rutiner	Leverantören ska ha dokumenterade rutiner för övervakning, upptäckt, analys, rapportering, eskalering, hantering av säkerhetshändelser och säkerhetsincidenter. Om incidenten i någon mån påverkar beställaren så ska beställaren inkluderas i dessa rutiner	Ska		

3.48	A.16.1.4 Bedömning av och beslut om informationssäkerhetshändelser	Leverantören ska bedöma och besluta ifall en informationssäkerhetshändelse ska klassas som en informationssäkerhetsincident. Om händelsen i någon mån påverkar beställaren så ska beställaren inkluderas i detta beslut.	Ska		
3.49	A.16.1.5 Hantering av informationssäkerhetsinciden ter	Leverantören ska ha rutiner för att hantera säkerhetsincidenter enligt gällande lagar och förordningar. Om incidenten i någon mån påverkar beställaren så ska en överenskommen och utpekad funktion hos beställaren inkluderas i dessa rutiner. Rutinerna ska granskas årligen.	Ska		
3.50	A.17.1.2 Införa kontinuitet för informationssäkerhet	Leverantören ska ha reservrutiner, reservlösningar och återstartsplaner som uppfyller beställarens krav på tillgänglighet (SLA).	Ska		
3.51	A.18.1.1 Identifiering av tillämplig lagstiftning och avtalsmässiga krav	Leverantören ska löpande och i samråd med beställaren arbeta för att leveransen i alla lägen följer de aktuella lagar, förordningar, regler och föreskrifter som ställs på beställarens verksamhet.	Ska		
3.52	A.18.1.4 Skydd av personlig integritet och personuppgifter	Leverantören ska utveckla och införa regler för skydd av personuppgifter med stöd i lagar och förordningar. Dessa regler ska kommuniceras till medarbetare hos leverantören som berörs av leveransen som hanterar personuppgifter.	Ska		
3.53	A.18.2.3 Granskning av teknisk efterlevnad	Beställaren ska i samråd med leverantören ha rätt att genomföra säkerhetsrevisioner av ingående delar i leveransen.	Ska		
3.54	A. 18.1.2 Immateriella rättigheter	Leverantören ska begära tillstånd innan information i system (texter, bilder etc.) eller tjänster återanvänds i andra sammanhang.	Ska		

Personuppgiftsbiträdesavtal

mellan _____ (nämnd/bolag), nedan kallad Personuppgiftsansvarig,

och _____ (leverantör), nedan kallad Personuppgiftsbiträde.

Detta Personuppgiftsbiträdesavtal är en bilaga till parternas Huvudavtal 20xx-xx-xx angående XX

---

med diarienummer XXX/XXXX.

*OBS Detta är endast en mall för att underlätta för Personuppgiftsansvarig att upprätta ett Personuppgiftsbiträdesavtal. Den som tecknar Huvudavtalet kan behöva ta kontakt med lokal dataskyddsorganisation inklusive lokal informationssäkerhetssamordnare för att göra nödvändiga anpassningar av detta Personuppgiftsbiträdesavtal. Till Personuppgiftsbiträdesavtalet hör **bilaga 1** med instruktion som ska fyllas i (obligatoriskt).*

1. Bakgrund

Enligt Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (”Dataskyddsförordningen”) ska det finnas ett skriftligt avtal mellan Personuppgiftsansvarig och Personuppgiftsbiträde avseende den behandling av personuppgifter som Personuppgiftsbiträdet ska utföra för Personuppgiftsansvarigs räkning.

Detta Personuppgiftsbiträdesavtal mellan Personuppgiftsansvarig och Personuppgiftsbiträde (nedan ”Parterna”) reglerar hur Personuppgiftsbiträdet får behandla personuppgifter för Personuppgiftsansvarigs räkning. Personuppgiftsbiträdesavtalet utgör en bilaga till Huvudavtalet, men utgör samtidigt ett självständigt avtal. I

händelse av motstridig lydelse mellan bestämmelserna om personuppgiftsbehandling i Personuppgiftsbiträdesavtalet och Huvudavtalet har Personuppgiftsbiträdesavtalet företräde. I fall av gällande standardavtalsklausuler för tredjelandsöverföring har dock standardavtalsklausulerna företräde i händelse av motstridig lydelse med detta Personuppgiftsbiträdesavtal eller Huvudavtalet.

2. Definitioner

Begreppen ”Personuppgiftsansvarig”, ”Personuppgiftsbiträde”,” samt andra begrepp i detta Personuppgiftsbiträdesavtal, som är relaterade till behandling av personuppgifter, ska tolkas och tillämpas i enlighet med vad som följer av Dataskyddsförordningen.

Med ”Standardavtalsklausuler” avses EU-kommissionens beslutade standardavtalsklausuler.

3. Behandling av personuppgifter

Allmänt om personuppgiftsbehandlingen

Personuppgiftsbiträdet och personer som agerar för Personuppgiftsbiträdets räkning får endast behandla personuppgifter i enlighet med Personuppgiftsbiträdesavtalet inklusive de skriftliga instruktioner som Personuppgiftsansvarig lämnar, samt ”Tillämplig lag” varmed avses gällande nationell och EU-lagstiftning avseende dataskydd som gäller för personuppgiftsbehandlingen inom ramen för Personuppgiftsbiträdesavtalet.

Om Personuppgiftsbiträdet finner att instruktioner är otydliga, i strid med Tillämplig lag eller saknas och Personuppgiftsbiträdet bedömer att nya eller kompletterande instruktioner är nödvändiga för att genomföra sina åtaganden ska Personuppgiftsbiträdet utan dröjsmål informera Personuppgiftsansvarig om detta och därefter invänta vidare instruktioner från Personuppgiftsansvarig.

Utöver de skyldigheter som Personuppgiftsbiträdet har enligt Tillämplig lag ska Personuppgiftsbiträdet även följa den uppförandekod eller certifiering som Personuppgiftsbiträdet har åtagit sig att följa.

Säkerhet vid personuppgiftsbehandling

Personuppgiftsbiträdet ska vidta alla åtgärder som krävs enligt artikel 32 Dataskyddsförordningen. Det innebär att Personuppgiftsbiträdet ska implementera och löpande säkerställa lämpliga tekniska och

organisatoriska åtgärder i enlighet med detta Personuppgiftsbiträdesavtal inklusive instruktioner och Tillämplig lag i syfte att skydda personuppgifter från 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. Personuppgiftsbiträdet ska systematiskt testa, undersöka och utvärdera de tekniska och organisatoriska åtgärder som ska säkerställa personuppgiftsbehandlingens säkerhet. Notera att lämpliga åtgärder även inkluderar Personuppgiftsbiträdets förmåga att upptäcka och hantera eventuell personuppgiftsincident.

Personuppgiftsbiträdet ska bistå Personuppgiftsansvarig genom lämpliga tekniska och organisatoriska åtgärder, så att Personuppgiftsansvarig kan fullgöra sin skyldighet enligt Tillämplig lag.

Personuppgiftsbiträdet ska bistå Personuppgiftsansvarig med att tillse att skyldigheterna enligt artiklarna 32-36 i Dataskyddsförordningen fullgörs, inklusive vara behjälplig med genomförandet av konsekvensbedömning avseende dataskydd.

Tredjelandsöverföring i samband med personuppgiftsbehandling

Personuppgiftsbiträdet ska säkerställa att personuppgifterna behandlas inom EU/EES. Personuppgiftsbiträdet får endast överföra personuppgifter till tredjeland (utanför EU/EES) om Personuppgiftsansvarig på förhand skriftligen godkänt sådan överföring och den är förenlig med Tillämplig lag. Se närmare instruktioner för tredjelandsöverföring i **bilaga 1**.

4. Registrerades rättigheter

Personuppgiftsansvarig ansvarar för att informera registrerade om personuppgiftsbehandlingen och för att tillvarata registrerades rättigheter enligt Tillämplig lag. Personuppgiftsbiträdet ska vid behov och utan onödigt dröjsmål bistå Personuppgiftsansvarig i hanteringen av en registrerads begäran om exempelvis registerutdrag eller radering (registrerades rättigheter i enlighet med kapitel III i Dataskyddsförordningen).

Om Personuppgiftsbiträdet tar emot en begäran från registrerad om utövande av sina rättigheter eller tillhörande frågor, ska Personuppgiftsbiträdet hänvisa den registrerade till Personuppgiftsansvarig samt utan onödigt dröjsmål informera Personuppgiftsansvarig.

5. Sekretess och tystnadsplikt

Personuppgiftsbiträdet och samtliga fysiska personer som arbetar under dess ledning ska behandla personuppgifterna under sekretess/tystnadsplikt och inte avslöja eller göra personuppgifter tillgängliga för tredje part, om inte detta har godkänts i förväg av Personuppgiftsansvarig eller krävs enligt Tillämplig lag eller föreläggande från tillsynsmyndighet.

Personuppgiftsbiträdet ska säkerställa att endast sådan personal som måste ha tillgång till personuppgifter för att kunna fullgöra Personuppgiftsbiträdets skyldigheter enligt Personuppgiftsbiträdesavtalet får tillgång till sådana personuppgifter. Personuppgiftsbiträdet ska säkerställa att all sådan personal är bunden av sekretess/tystnadsplikt, antingen genom lag eller avtal, sådant avtal ska åtminstone motsvara det krav på sekretess/tystnadsplikt som följer av detta Personuppgiftsbiträdesavtal. Personuppgiftsbiträdet ska också säkerställa att personalen förstår innebörden av sekretess-/tystnadspliktsåtagandet.

Sekretess- och tystnadspliktsåtagandet gäller även under tid efter det att Personuppgiftsbiträdesavtalet i övrigt upphört att gälla.

6. Granskning, revision och kontroll

Personuppgiftsbiträdet ska bistå Personuppgiftsansvarig vid granskning inbegripet inspektion som tillsynsmyndighet kan komma att genomföra av Personuppgiftsansvarig. Personuppgiftsbiträdet ska utan dröjsmål informera Personuppgiftsansvarig om eventuella kontakter med tillsynsmyndighet. Personuppgiftsbiträdet får inte företräda Personuppgiftsansvarig eller på annat sätt agera för Personuppgiftsansvarigs räkning gentemot tillsynsmyndighet, eller annan tredje part, utan skriftligt medgivande från Personuppgiftsansvarig.

Personuppgiftsbiträdet ska ge Personuppgiftsansvarig tillgång till all information som krävs för att visa att behandling av personuppgifter uppfyller Tillämplig lag jämte de villkor som enligt detta Personuppgiftsbiträdesavtal gäller för personuppgiftsbehandling.

Personuppgiftsbiträdet förbinder sig att följa eventuella beslut från tillsynsmyndighet avseende behandlingen av personuppgifter för Personuppgiftsansvarigs räkning enligt detta Personuppgiftsbiträdesavtal.

Personuppgiftsansvarig får själv eller genom tredje part genomföra revision i skälig utsträckning eller på förekommen anledning gentemot Personuppgiftsbiträdet eller på annat sätt kontrollera att Personuppgiftsbiträdets behandling av personuppgifter följer detta Personuppgiftsbiträdesavtal. Vid sådan revision eller kontroll ska

Personuppgiftsbiträdet ge Personuppgiftsansvarig den assistans som behövs för genomförande av den aktuella åtgärden.

För det fall att registrerade, tillsynsmyndighet eller annan tredje part begär information från någon av Parterna som på något sätt innefattar behandling av personuppgifter enligt detta Personuppgiftsbiträdesavtal ska Parterna samverka och utbyta information i nödvändig utsträckning.

7. Personuppgiftsbiträdets anlitande av underbiträde

Personuppgiftsbiträdet får inte anlita ett annat personuppgiftsbiträde (nedan ”Underbiträde”) för behandling av personuppgifter för Personuppgiftsansvarigs räkning utan ett i förväg inhämtat skriftligt godkännande från Personuppgiftsansvarig.

Om Personuppgiftsbiträdet anlitar ett Underbiträde för behandlingen av personuppgifter, ska Personuppgiftsbiträdet ålägga genom ett skriftligt avtal Underbiträdet motsvarande skyldigheter i fråga om dataskydd vid behandling av personuppgifter som gäller för Personuppgiftsbiträdet enligt detta Personuppgiftsbiträdesavtal. Om Underbiträdet inte fullgör sina skyldigheter i fråga om dataskydd vid behandling av personuppgifter ska Personuppgiftsbiträdet vara fullt ansvarig gentemot Personuppgiftsansvarig för utförandet av det Underbiträdets skyldigheter.

I det fall Personuppgiftsbiträdet och Underbiträdet har ingått gällande Standardavtalsklausuler om tredjelandsöverföring har Standardavtalsklausulerna företräde i händelse av motstridig lydelse med detta Personuppgiftsbiträdesavtal.

De av Personuppgiftsansvarig godkända Underbiträdena framgår av instruktionen i **bilaga 1.**

Personuppgiftsansvarig eller av denne anlitad annan part har rätt till assistans från Personuppgiftsbiträdet vid revision och kontroll avseende behandling av personuppgifterna som utförs genom av denne anlitade Underbiträden.

8. Personuppgiftsincident

För det fall Personuppgiftsbiträdet misstänker alternativt upptäcker någon 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 (”Personuppgiftsincident”) ska Personuppgiftsbiträdet omedelbart

undersöka Personuppgiftsincidenten och vidta lämpliga åtgärder för att läka Personuppgiftsincidenten och förhindra en upprepning.

Personuppgiftsbiträdet ska utan onödigt dröjsmål efter att ha fått vetskap om Personuppgiftsincidenten tillhandahålla Personuppgiftsansvarig en beskrivning av Personuppgiftsincidenten och därefter löpande förse Personuppgiftsansvarig med information om Personuppgiftsincidenten.

Beskrivningen av Personuppgiftsincidenten ska åtminstone:

a) beskriva Personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgifter som berörs,

b) förmedla namnet på och kontaktuppgifterna till dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas,

c) beskriva de sannolika konsekvenserna av Personuppgiftsincidenten, och

d) beskriva de åtgärder som Personuppgiftsbiträdet har vidtagit eller föreslagit för att åtgärda Personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

9. Ansvar

Vid ersättning för skada i samband med personuppgiftsbehandling som, genom fastställd dom, förlikning eller annat beslut, utgått till den registrerade på grund av överträdelse av bestämmelse i Tillämplig lag ska artikel 82 Dataskyddsförordningen tillämpas, jämte 7 kap. 1 § lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Vad gäller påförd administrativ sanktionsavgift enligt artikel 83 Dataskyddsförordningen och 6 kap. 2 och 3 §§ lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, ska den bäras av den av Parterna som påförts en sådan avgift.

Ansvar enligt denna punkt 9 st 1 och st 2 gäller före andra avtalsbestämmelser i Huvudavtalet om fördelning mellan Parterna av krav sinsemellan såvitt avser registrerads ersättning och sanktionsavgift.

Vad gäller skadeståndsansvar till följd av en parts avtalsbrott mot Personuppgiftsbiträdesavtalet gäller Huvudavtalets bestämmelser om påföljder.

Om endera part får kännedom om omständighet som kan leda till skada för motparten ska parten omedelbart informera motparten om förhållandet och aktivt arbeta tillsammans med motparten för att förhindra och minimera sådan skada.

10. Ersättning för utförande av Personuppgiftsbiträdets uppdrag

Personuppgiftsbiträdet har inte rätt till ersättning under detta Personuppgiftsbiträdesavtal. Personuppgiftsbiträdets rätt till ersättning i övrigt är uteslutande reglerat i Huvudavtalet.

11. Personuppgiftsbiträdesavtalets giltighetstid

Detta Personuppgiftsbiträdesavtal träder ikraft på dagen för dess undertecknande och gäller så länge som Personuppgiftsbiträdet behandlar personuppgifter för Personuppgiftsansvarigs räkning som en del av åtagandet att leverera tjänst i enlighet med Huvudavtalet, eller vid den senare tidpunkt då personuppgifterna i sin helhet är raderade eller återlämnade enligt Personuppgiftsansvarigs instruktion.

12. Upphörande av behandling av personuppgifter

Vid upphörande av behandling av personuppgifter enligt Personuppgiftsbiträdesavtalet ska Personuppgiftbiträdet radera eller återlämna alla personuppgifter i enlighet med Personuppgiftsansvarigs instruktioner samt säkerställa att inga personuppgifter eller kopior därav är kvar i Personuppgiftsbiträdets besittning. Radering eller återlämnande ska utföras senast inom trettio (30) dagar från upphörandet av personuppgiftsbehandlingen.

Ovan utgör en precisering av eventuell reglering i Huvudavtalet avseende återlämning eller radering av data. I fall av motstridig lydelse avseende radering eller återlämning av data i Huvudavtalet och denna punkt 12 ska denna punkt ha företräde.

Om personuppgifterna återlämnas till Personuppgiftsansvarig ska det ske i ett öppet och standardiserat format som möjliggör återanvändning av personuppgifterna för liknande ändamål.

13. Ändringar och tillägg

Personuppgiftsansvarig får, i den mån så erfordras för att krav som följer av Tillämplig lag ska kunna tillgodoses, skriftligen ändra innehållet i detta Personuppgiftsbiträdesavtal. Sådan skriftlig ändring träder ikraft

trettio (30) dagar efter det att meddelande härom översänts, om inte längre tidsfrist anges i meddelandet eller annan tidsfrist föranleds av Tillämplig lag.

Andra ändringar av och/eller tillägg till detta Personuppgiftsbiträdesavtal ska vara skriftliga och undertecknade av båda Parterna för att vara bindande.

14. Tvist

Tvist angående tolkning eller tillämpning av detta Personuppgiftsbiträdesavtal ska avgöras enligt svensk lag och av svensk allmän domstol.

15. Övrigt

Parterna ska inom ramen för Personuppgiftsbiträdesavtalet utse varsin kontaktperson.

Meddelanden inom ramen för Personuppgiftsbiträdesavtalet ska skickas till respektive parts kontaktperson för Personuppgiftsbiträdesavtalet.

Detta Personuppgiftsbiträdesavtal har upprättats i två originalexemplar, varav Parterna tagit var sitt.

Ort och datum	Ort och datum
Nämndens/bolagets underskrift	Leverantörens underskrift
Namnförtydligande	Namnförtydligande

Bilaga 1 - Instruktion till Personuppgiftsbiträdesavtal

All kursiverad text i detta dokument utgör vägledning för hur instruktionen ska fyllas i. När ni fyllt i dokumentet säkerställ att sådan text tas bort och att ni har fyllt i enligt anvisningarna.

Utöver vad som redan framgår av Personuppgiftsbiträdesavtalet ska Personuppgiftsbiträdet följa gällande instruktioner vid behandling av personuppgifter för Personuppgiftsansvarigs räkning.

1. Ändamål för behandling av personuppgifter

Personuppgiftsbiträdet får behandla personuppgifter för Personuppgiftsansvarigs räkning för att tillhandahålla tjänsten/er i enlighet med Huvudavtalet. Personuppgiftsbiträdet ska bara behandla personuppgifterna för ändamålet att uppfylla sina åtaganden i enlighet med Huvudavtalet.

Här ska ni ange det specifika ändamålet med Personuppgiftsbiträdets behandling av personuppgifter d.v.s. syftet med den tjänst som ska utföras enligt Huvudavtalet, t.ex. tillhandahålla support och/eller applikations- och förvaltningsstöd: *(fyll i)*

När leverantören utför tjänster enligt Huvudavtalet kan leverantören komma att behandla personuppgifter som ett personuppgiftsbiträde, men i vissa fall som en personuppgiftsansvarig. Precisera här enbart de tjänster i Huvudavtalet som leverantören utför som ett personuppgiftsbiträde.

2. Kategori av personuppgifter

Nedan ska ni beskriva de typer av personuppgifter som behandlas inom ramen för Personuppgiftsbiträdesavtalet. I det följande lämnas ett antal exempel, men ni ska ange preciserat alla de typer av personuppgifter (direkta och indirekta) som Personuppgiftsbiträdet får behandla.

Personuppgiftsbiträdet får för Personuppgiftsansvarigs räkning behandla följande kategorier av personuppgifter: *(fyll i)*

Kontaktuppgifter och liknande som t. ex.

- *personlig information som namn, födelsedatum, kön, personnummer, organisationsnummer vid enskild firma, titel/funktion, anställningsidentitet, fotografi, IP-adress,*

- *kontaktuppgifter*
- *annat inklusive indirekta personuppgifter*

Integritetskänsliga och särskilt skyddsvärda personuppgifter som t. ex.

- *personnummer eller samordningsnummer*
- *uppgifter om lagöverträdelser*
- *personuppgifter som omfattas av sekretess eller tystnadsplikt som t.ex. behandlas inom ramen för ärendehandläggning eller utredning kopplat till en individ*
- *skyddade personuppgifter*
- *uppgifter relaterade till en registrerads anställningsförhållanden t. ex. värdeomdömen*
- *bankkontonummer etcetera*
- *säkerhetsuppgifter som inloggningsuppgifter, information om anställdas it-hantering såsom behörigheter och loggar m m samt övervakningsuppgifter av olika slag etcetera*
- *andra integritetskänsliga eller särskilt skyddsvärda personuppgifter inklusive indirekta personuppgifter*

Med känsliga personuppgifter avses personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om fysisk persons sexualliv eller sexuella läggning.

Personuppgiftsbiträdet får behandla följande känsliga personuppgifter: *(fyll i)*

Vid behandling av känsliga och/eller särskilt skyddsvärda personuppgifter ska Personuppgiftsbiträdet införa sådana ytterligare åtgärder som krävs för skydd av sådana personuppgifter, se punkt 6.

3. Kategorier av registrerade

Ange de kategorier av registrerade vars personuppgifter kommer att behandlas är*: (fyll i)*

Några exempel ges som följer; sökande, registrerade relaterade till vård och omsorg (d.v.s. brukare, patienter och deras anhöriga), invånare, stadens anställda, leverantörers anställda och konsulter, fastighetsägare, kunder, förtroendevalda politiker, elever, barn, vårdnadshavare, äldre, funktionsnedsatta m fl.

4. Plats för behandling

Personuppgiftsansvarig ska här beskriva
a) var personuppgifter får behandlas geografiskt, och
b) om tredjelandsöverföring är tillåten, beskriv det rättsliga stödet för den aktuella överföringen i enlighet med kap. V i Dataskyddsförordningen.

Med överföring av personuppgifter till tredjeland avses all personuppgiftsbehandling som kan komma att ske i ett tredjeland t. ex. då personuppgifter överförs till eller nås genom fjärråtkomst från tredjeland. Notera att ett bolags ägarförhållanden kan avgöra plats för behandling, detta som en följd av att exempelvis amerikansk s k problematisk lagstiftning kan möjliggöra för exempelvis amerikanska underrättelsemyndigheter att i vissa fall ställa krav på en utlämnandebegäran till ett amerikanskägt bolag, varvid en behandling kan komma att ske i USA.

Personuppgiftsbiträdet får behandla personuppgifterna på följande geografiska platser: *(fyll i, lista de länder i vilka personuppgifterna kommer att behandlas)*

Europeiska Unionen eller Europeiska Ekonomiska Samarbetsområdet (EES): *(fyll i)*

Tredjeland utanför EU/EES: *(fyll i)*

Innan tredjelandsöverföring får ske ska Parterna ha säkerställt att det finns ett rättsligt stöd för överföringen i form av exempelvis *adekvansbeslut* av EU-kommissionen om tillåten överföring, alternativt säkerställt ingående av *Standardavtalsklausuler kompletterat av genomförd riskanalys för tredjelandsöverföring* (s k Transfer Impact Assessment , TIA, i enlighet med Europeiska dataskyddsstyrelsens rekommendation[1]). Beskriv rättsligt stöd för varje tredjelandsöverföring som sker: *(fyll i)*

Ange land/rättsligt stöd för överföring som exempelvis EU-kommissionens adekvansbeslut eller Standardavtalsklausulerna jämte riskanalys för tredjelandsöverföring, TIA. Om ni inte tredjelandsöverför några personuppgifter kan detta stycke utgå.

Bilägg ingångna giltiga Standardavtalsklausuler mellan Personuppgiftsansvarig och Personuppgiftsbiträde, samt genomförd riskanalys för tredjelandsöverföring, TIA. Sker tredjelandsöverföringen

[1] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 Adopted on 18 June 2021

mellan Personuppgiftsbiträde och dess Underbiträde är Personuppgiftsbiträdet ansvarig för ingåendet av Standardavtalsklausulerna med Underbiträdet och ska på begäran uppvisa dessa för Personuppgiftsansvarig.

5. Underbiträden

I nedan tabell ska Personuppgiftsbiträdet ange godkända Underbiträden och de land/länder anges där Underbiträdet behandlar personuppgifter. Kom ihåg att behandling i ett land även inbegriper fjärråtkomst från det landet, liksom att Underbiträdets ägarförhållanden i vissa fall kan avgöra plats för behandling på så sätt att exempelvis ett amerikanskägt Underbiträde i vissa fall kan få en utlämnandebegäran från amerikanska underrättelsemyndigheter varvid en behandling kan komma att ske i USA. Fyll i tabellen med korrekt lämnad information från Personuppgiftbiträdet:

Följande Underbiträden hos Personuppgiftsbiträdet får behandla personuppgifter för Personuppgiftsansvarigs räkning:*(fyll i)*

Underbiträde	**Behandling sker i (land)**

6. Säkerhet; tekniska och organisatoriska åtgärder

Vid ifyllnad av denna punkt bör kontakt tas med er lokala informationssäkerhetssamordnare (ISAM).

De personuppgifter som behandlas av Personuppgiftsbiträdet ska skyddas på det sätt som anges i Personuppgiftsbiträdesavtalet (inklusive tillkommande skriftliga instruktioner från Personuppgiftsansvarig) jämte Tillämplig lag.

Artikel 32 p 1 Dataskyddsförordningen anger ”Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt

a) pseudonymisering och kryptering av personuppgifter,
b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,
c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,
d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.”

Personuppgiftsbiträdet ska vidta och implementera följande beslutade tekniska och organisatoriska skyddsåtgärder enligt artikel 32 Dataskyddsförordningen: *(fyll i)*

Ange här de säkerhetskrav som gäller för leverans av tjänsten enligt Huvudavtalet med bilagor - som exempelvis bilaga med säkerhetskrav i upphandlingsdokumentationen, bilaga med Stockholms stads riktlinjer för informationssäkerhet inklusive tillhörande tillämpningsanvisningar, eller bilaga med Stockholms stads policy för skyddade personuppgifter.
För det fall en informationsklassning har gjorts inför upphandlingen och utgjort en del av kraven i upphandlingsdokumentationen kan ni hänvisa till informationsklassningen. I annat fall kan ni med beaktande av upphandlingslagstiftningen beskriva en precisering av de i upphandlingsdokumentationen ställda säkerhetskraven d.v.s. de tekniska och organisatoriska åtgärderna.

Har Personuppgiftsbiträdet ytterligare preciserande beskrivningar av implementerade tekniska och organisatoriska åtgärder kan de redovisas här.

Personuppgiftsbiträdet ska vid behov för att efterleva Tillämplig lag korrigera de implementerade tekniska och organisatoriska åtgärderna efter avstämning med Personuppgiftsansvarig. Notera att avtalsändringar regleras i punkt 13 Personuppgiftsbiträdesavtalet.

7. Återlämning eller radering av personuppgifter

Här anges specifika instruktioner om hur personuppgifter ska raderas eller återlämnas till Personuppgiftsansvarig*: (fyll i)*

8. Ytterligare instruktioner från Personuppgiftsansvarig

Personuppgiftsbiträdet ska se till att samtliga personer som behandlar personuppgifter enligt detta Personuppgiftsbiträdesavtal hos Personuppgiftsbiträdet har fått erforderlig utbildning om Tillämplig lag

gällande personuppgiftsbehandling. Personuppgiftsbiträdet ska säkerställa att endast personer som behöver ha tillgång till personuppgifterna för utförandet av sitt arbete har tillgång till personuppgifterna.

Ange eventuella övriga tillkommande instruktioner för behandlingen, såsom exempelvis krav avseende gallring: *(fyll i)*

9. Varaktighet

Instruktionen gäller så länge som Personuppgiftsbiträdet behandlar personuppgifter för Personuppgiftsansvarigs räkning enligt Personuppgiftsbiträdesavtalet, inom ramen för utförandet av tjänsten enligt Huvudavtalet, eller till den tidpunkt då instruktionen ändras.

Personuppgiftsansvarig kan göra ändringar i och tillägg till denna Instruktion i enlighet med vad som följer av punkt 13 Personuppgiftsbiträdesavtalet.