Bilaga 1 Instruktion om hantering av personuppgifter

Project Office behandlar personuppgifter för följande ändamål:	Tillhandahålla tjänsten
Kategorier av personuppgifter Kategorier av personuppgifter som kommer behandlas av Project Office omfattar:	Inga känsliga personuppgifter Namn, personnummer, e-post, telefonnummer. Vid andra personuppgifter förväntas kunden meddela Project Office dessa.
Kategorier av registrerade Samtliga kategorier av registrerade vars uppgifter kommer behandlas av Project Office är följande:	Project Offices kunders kunder samt i vissa fall Project Offices kunders anställda. Vid andra kategorier av registrerade förväntas kunden meddela Project Office dessa.
Gallringstid Den gallringstid som gäller avseende när personuppgifterna som behandlas av Project Office ska gallras är följande:	De personuppgifter som behandlas inom ramen för Project Offices tillhandahållande av Tjänsten sparas endast under den period som avtalet gäller och raderas senast 1 månad därefter eller tidigare om kunden väljer att radera uppgifterna.
Praktisk hantering Specificering av hur behandling ska gå till är följande:	Personuppgifterna behandlas enbart i den utsträckning det är nödvändigt för Project Offices tillhandahållande av tjänsten. Detta innebär t.ex. Överföring till backuper Lagring nödvändig för tjänsten
Tekniska och organisatoriska åtgärder:	
NDA	Vi säkerställer att anställda och konsulter har ingått sekretessavtal
Åtkomstkontroll	Personuppgiftsbiträden ska implementera och säkerställa efterlevnad av nödvändiga och lämpliga tekniska och organisatoriska åtgärder för att skydda behandlingen av personuppgifter mot obehörig åtkomst, förstörelse och förändring. För att förhindra att obehöriga personer får åtkomst till databehandlingssystem där personuppgifter behandlas (fysisk åtkomstkontroll) ska Project Office vidta åtgärder för att förhindra fysisk åtkomst säkrade lokaler. För att förhindra att databehandlingssystem

	används utan tillstånd (systemåtkomstkontroll) kan följande tillämpas beroende på de specifika tjänster som beställs: • autentisering via lösenord • dokumenterade autentiseringsprocesser • dokumenterade ändringshanteringsprocesser • loggning av åtkomsten på flera nivåer.
Loggning av åtkomst till personuppgifter **Brandväggar och antivirusskydd**	För att säkerställa att personer med rätt att använda ett databehandlingssystem endast har åtkomst till de personuppgifter till vilka de har åtkomstprivilegier, och att personuppgifter inte får läsas, kopieras, modifieras eller avlägsnas utan tillstånd under behandlingen och/eller efter lagringen (uppgiftsåtkomstkontroll), är personuppgifter endast åtkomliga och hanterbara av personal med rätt behörighet, den direkta åtkomsten för databasförfrågningar är begränsad och åtkomsträttigheterna till applikationen fastställs och verkställs.
Kryptering av datakommunikation	För att säkerställa att personuppgifter inte kan läsas, kopieras eller modifieras utan tillstånd under elektronisk överföring eller transport och att det är möjligt att kontrollera och fastställa till vilka enheter överföringen av personuppgifter med dataöverföringshjälpmedel är tänkt (överföringskontroll) kommer Project Office att uppfylla följande krav: Om inte annat föreskrivs för tjänsterna kan data utanför tjänstemiljön vara krypterad.
Auktorisation och behörigheter	För att säkerställa att det är möjligt att kontrollera och fastställa om och av vem personuppgifter har förts in i databehandlingssystem, modifierats eller avlägsnats (inmatningskontroll) ska Project Office uppfylla följande krav: • källan till personuppgifterna står under Kundens kontroll och personuppgifternas integrering i systemet hanteras genom säker filöverföring (dvs. via webbtjänster eller läggs in i applikationen) från Kunden.
Backup	För att säkerställa att personuppgifter skyddas från förstörelse eller förlust, för tjänster med Project Office som värd gäller följande: • säkerhetskopiering kan ske regelbundet men

	att aktivera detta är kundens ansvar • Det är kundens ansvar att säkerställa att säkerhetskopiering sker på ett sätt som uppfyller alla juridiska krav.
Service och reparationer av enheter där personuppgifter lagras	Certifierad radering av hårdvara
Separering av miljöer	För att säkerställa att personuppgifter som samlas in i olika syften kan behandlas separat segregeras uppgifter från olika Project Office-kunders miljö logiskt i Project Offices system. Den personuppgiftsansvariga har det slutgiltiga ansvaret att bedöma vilken säkerhetsåtgärd som måste vidtas. När den allmänna dataskyddsförordningen (GDPR) träder i kraft den 25 maj 2018 kommer personuppgiftsbiträdet dock att ha ett eget ansvar att skydda att nödvändiga säkerhetsåtgärder för behandlingen implementeras, liksom vid behov ytterligare tekniska åtgärder och säkerhetsåtgärder. Om dessa ytterligare tekniska och organisatoriska åtgärder ökar kostnaden för personuppgiftsbiträdet ska detta betalas separat av den personuppgiftsansvariga i enlighet med detta Biträdesavtal.
Granskningsrättigheter	Project Office ska på Kundens begäran tillhandahålla Kunden intyg om efterlevnad av dataskydd och molnsäkerhet som är tillämpliga på tjänsterna. Kunden får granska Project Offices efterlevnad av villkoren i avtalet och detta databehandlingsavtal, högst en gång per år. Kunden får utföra granskningar av tjänstens datasystem som behandlar personuppgifter om det krävs enligt lagar som gäller för Kunden. Om en tredje part ska utföra granskningen måste den tredje parten avtalas ömsesidigt av Kunden och Project Office och underteckna ett skriftligt sekretessavtal som är godtagbart för Project Office innan granskningen genomförs. För att begära en granskning måste Kunden lämna en detaljerad granskningsplan minst två veckor före den föreslagna granskningsdagen till Project Office, med en beskrivning av den föreslagna omfattningen, varaktigheten och startdatumet för granskningen. Project Office

	ska läsa granskningsplanen och informera Kunden om eventuella bekymmer eller frågor (t.ex. en begäran om information som skulle kunna äventyra Project Offices säkerhet, integritet eller anställningspolicyer). Kunden ska tillhandahålla Project Office eventuella granskningsrapporter som genereras i samband med en granskning enligt denna paragraf, om det inte är förbjudet enligt lag. Kunden får endast använda granskningsrapporten för att uppfylla sina lagstadgade granskningskrav och/eller bekräfta efterlevnaden av kraven i avtalet och detta databehandlingsavtal. Granskningsrapporterna är parternas konfidentiella information enligt villkoren i detta databehandlingsavtal. Granskningar sker på Kundens bekostnad. En eventuell begäran om att Project Office ska erbjuda assistans vid en granskning anses vara en separat tjänst om denna granskningsassistans kräver användning av andra eller ytterligare resurser. Project Office kommer att söka Kundens skriftliga tillstånd och samtycke till att betala eventuella tillhörande åtgärder innan sådan granskningsassistans utförs.
Incidenthantering och meddelande om säkerhetsbrott	Project Office utvärderar och reagerar på incidenter som skapar en misstanke om obehörig åtkomst till eller hantering av personuppgifter. Project Office informeras om sådana incidenter och definierar, beroende på verksamhetens art, eskaleringsvägar och responsteam för att hantera incidenterna. Project Office kommer att samarbeta med Kunden, med rätt tekniska team och, vid behov, med brottsbekämpande myndigheter för att reagera på incidenten. Målet med incidentresponsen är att återställa tjänstemiljöns sekretess, integritet och tillgänglighet, och att fastställa bakomliggande orsaker och korrigeringsåtgärder. I denna paragraf avses med ”säkerhetsbrott” ett felaktigt tillförskansande av personuppgifter som finns i Project Offices system eller tjänstemiljön som äventyrar dessa uppgifters säkerhet, sekretess eller integritet. Project Offices operativa personal har instruktioner om hur de ska reagera på incidenter där hanteringen av personuppgifter kan ha varit obehörig, inklusive snabb och skälig rapportering till Project Office, eskaleringsförfaranden och spårbarhetssystem

för att säkra relevanta bevis. Project Office ska informera Kunden utan oskäligt dröjsmål från det att ett säkerhetsbrott upptäcktes, om Project Office fastställer att personuppgifter har varit föremål för ett säkerhetsbrott eller andra omständigheter där Kunden är skyldig att lämna ett meddelande enligt gällande lag, om inte annat krävs enligt lag. Project Office ska skyndsamt utreda eventuella säkerhetsbrott och vidta skäliga åtgärder för att identifiera deras bakomliggande orsak(er) och förhindra att de upprepas.
När information samlas in eller blir tillgänglig på annat sätt ska Project Office, om det inte är förbjudet enligt lag, förse Kunden med en beskrivning av säkerhetsbrottet, den typ av uppgifter som var föremål för brottet och annan information som Kunden skäligen kan begära när det gäller de berörda registrerade. Parterna enas om att i god tro samordna sin utveckling av innehållet av eventuella tillhörande offentliga uttalanden eller nödvändiga meddelanden som rör de berörda registrerade.

Återlämnande och radering av personuppgifter efter tjänsternas upphörande eller på Kundens begäran

Efter detta Biträdesavtals upphörande och beroende på vad den personuppgiftsansvariga beslutar ska personuppgiftsbiträdet, och eventuella underpersonuppgiftsbiträden, antingen återlämna eller på annat sätt göra Kundens personuppgifter och kopior tillgängliga för hämtning i tjänstemiljön. Efter återlämnandet av uppgifterna, eller enligt annan överenskommelse, ska Project Office skyndsamt radera eller på annat sätt göra alla kopior av personuppgifterna otillgängliga från produktionstjänstemiljön, om det inte krävs enligt lag.

Garantier och skadeslöshet

Kunden garanterar att användningen av tjänsten inte ska missbrukas. Vid tillämpningen av denna paragraf ska missbruk avse att (i) agera i strid mot gällande lagar om personuppgifter och datasäkerhet, (ii) sprida information som kan betraktas som olaglig eller som är avsedd att användas för olagliga aktiviteter, (iii) oansvarigt sprida insamlade eller sammanställda personuppgifter eller (iv) på annat sätt engagera sig i handlingar som kan orsaka skada på Project Office, Project Offices system eller Project Offices andra kunder.