Bilaga 1 - [Mall för] Personuppgiftsansvariges Instruktion för Behandling av Personuppgifter

[Gulmarkerad text inom hakparenteser tas bort inför att Personuppgiftsbiträdesavtal upprättas.]

[Observera att om Personuppgiftsbiträdet ska utföra flera Behandlingar av Personuppgifter åt den Personuppgiftsansvarige för olika ändamål, t.ex. dels tillhandahålla ett IT-system, dels tillhandahålla support och service avseende systemet, ska Instruktionen specificera vad som gäller för respektive Behandling.]

Utöver vad som redan framgår av Personuppgiftsbiträdesavtalet ska Personuppgiftsbiträdet även följa nedanstående Instruktion:

1. Ändamålet, föremålet och arten
1 a. Föremålet för Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige är att: [Ange övergripande det huvudsakliga syftet med Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige, t.ex. tillhandahållande av ett HR-verktyg för löneadministration, en molntjänst för lagring av verksamhetsdata eller ett system för övervakning av inpassering till kontorslokaler.] 1 b. Ändamålet med Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige är att: [Ange ändamålet med Behandlingen, dvs. varför Personuppgiftsbiträdet ska Behandla Personuppgifterna åt den Personuppgiftsansvarige - vad är syftet med Behandlingen? Exempel på ändamål är att administrera utbetalning av löner och andra förmåner till medarbetare, att lagra informationstillgångar på ett säkert och kostnadseffektivt sätt eller att motverka olovlig inpassering i kontorslokaler. Beskrivningen ska vara så pass fullständig att externa parter (t.ex. en tillsynsmyndighet) kan förstå innehållet och riskerna med den Behandling som anförtrotts Personuppgiftsbiträdet.] 1 c. Personuppgiftsbiträdets Behandling av Personuppgifter på uppdrag av den Personuppgiftsansvarige avser huvudsakligen följande behandlingsåtgärder (Behandlingens art eller natur): [Ange Behandlingens art, dvs. vilka behandlingsåtgärder som Personuppgiftsbiträdet ska utföra åt den Personuppgiftsansvarige. Exempel på behandlingsåtgärder är insamling, lagring, läsning, strukturering, överföring osv.]
2. Behandlingen omfattar följande typer av Personuppgifter
Personuppgiftsbiträdet har rätt att behandla följande typer av Personuppgifter för den Personuppgiftsansvariges räkning: [Ange vilka typer av Personuppgifter som Personuppgiftsbiträdet har rätt att behandla åt den Personuppgiftsansvarige, t.ex. namn, e-postadress, postadress, telefonnummer, medlemsnummer, IP-adress, bilder, rörliga bilder, hälsouppgifter osv.]

3. Behandlingen omfattar vissa kategorier av Registrerade

Personuppgiftsbiträdet har rätt att Behandla Personuppgifter avseende följande kategorier av Registrerade:

[Ange vilka kategorier av Registrerade som Personuppgiftsbiträdet har rätt att behandla Personuppgifter om, t.ex. anställda, konsulter, patienter, brukare, närstående, elever, vårdnadshavare osv.]

4. Ange särskilda hanteringskrav vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet

Personuppgiftsbiträdet ska iaktta följande hanteringskrav vid Behandlingen av Personuppgifter åt den Personuppgiftsansvarige:

[Exempel på hanteringskrav är att personuppgifter ska gallras efter en viss angiven tidsperiod eller att säkerhetskopior inte får sparas längre än en viss angiven tidsperiod. Även krav på rutiner kring behörighetshantering kan anges här.]

5. Ange de särskilda tekniska och organisatoriska säkerhetsåtgärder som gäller för Personuppgiftsbiträdets Behandling av Personuppgifter

Personuppgiftbiträdet ska vidta följande säkerhetsåtgärder vid Behandlingen av Personuppgifterna:

[För att den Personuppgiftsansvarige ska kunna bedöma vilka säkerhetsåtgärder som Personuppgiftsbiträdet behöver vidta, behöver Personuppgiftsbiträdet redovisa teknisk dokumentation och systemspecifikation avseende aktuell tjänst eller system som klargör hur Personuppgifter hanteras och skyddas inom ramen för tjänsten eller systemet. Relevant information kan även framgå av Personuppgiftsbiträdets integritetspolicy (Privacy Policy). Utifrån dokumentationen kan den Personuppgiftsansvarige bedöma vilka åtgärder som ev. behöver anpassas eller kompletteras med för att uppnå en tillräcklig skyddsnivå för Personuppgifterna i syfte att bevara skyddet för Registrerades personliga integritet. Den här informationen kan mycket väl framgå av en särskild bilaga.

Samtliga tekniska och organisatoriska säkerhetsåtgärder som den Personuppgiftsansvarige kräver att Personuppgiftsbiträdet vidtar ska anges i detta avsnitt, ev. med hänvisning till en eller flera bilagor. Kravens närmare innehåll och utformning fastställs utifrån den Personuppgiftsansvariges risk- och sårbarhetsanalyser, t.ex. informationssäkerhetsklassning eller konsekvensbedömning avseende dataskydd enligt artikel 35 i dataskyddsförordningen, samt genom dialog med Personuppgiftsbiträdet. Säkerhetsåtgärderna ska vara dimensionerade efter Behandlingens art, omfattning och ändamål samt riskerna för de Registrerades integritet.

Åtgärderna kan exempelvis anges under följande underrubriker: Organisatoriska säkerhetsåtgärder, Säkerhetsåtgärder avseende personer, Fysiska säkerhetsåtgärder och Tekniska säkerhetsåtgärder (se ISO/IEC 27002).

Organisatoriska säkerhetsåtgärder kan avse krav gällande t.ex. ansvarsfördelning och roller, styrande dokument, risk- och incidenthantering, revision och annan uppföljning osv.

Säkerhetsåtgärder gällande personer kan avse krav på t.ex. sekretessåtagande, utbildning, arbete på distans, incidentrapportering osv.

Fysiska säkerhetsåtgärder kan avse krav avseende t.ex. utrustning, inpassering, övervakning av lokaler, lokalisering och skydd av hårdvara osv.

Tekniska säkerhetsåtgärder kan avse krav på t.ex. pseudonymisering av data, kryptering, systemövervakning samt tekniska metoder för säkerställande av sekretess, tillgänglighet, robusthet, återställande efter säkerhetsincident, loggning osv.]

6. Ange särskilda krav på Loggning vad gäller Behandling av Personuppgifter samt vilka som ska ha tillgång till dem

Personuppgiftsbiträdet ska iaktta följande krav avseende loggning av användaraktivitet och logghantering:

[Kraven kan t.ex. avse vad som ska framgå av loggarna, vilka som får ha tillgång till dem och hur länge de ska sparas.]

7. Lokalisering och överföring av Personuppgifter till Tredje land

Personuppgiftsbiträdet ska iaktta följande krav avseende lokalisering av Personuppgifter:

Personuppgiftsbiträdet har endast rätt att behandla Personuppgifterna på följande plats/er:

- [Ange plats/er för Behandlingen (postadress, land).]

Om den Personuppgiftsansvarige inte har gett anvisningar om överföring av Personuppgifter till ett Tredje land i Instruktionen, har Personuppgiftsbiträdet inte rätt att göra en sådan överföring.

Personuppgiftsbiträdet ska iaktta följande krav avseende överföring av Personuppgifter till Tredje land:

- [Ange ev. Instruktioner för överföring av Personuppgifter till Tredje land enligt följande exempel. För ändamålet xyz har Personuppgiftsbiträdet rätt att föra över Personuppgifter i form av xyz till xyzlandet för Behandling i form av xyz av Underbiträdet xyz. Rättslig grund för överföringen är xyz i kapitel V i Dataskyddsförordningen.]

8. Behandlingens varaktighet

[Ange tidsperioden, eller de kriterier som används för att fastställa tidsperioden, under vilken Personuppgiftsbiträdet får Behandla Personuppgifter åt den Personuppgiftsansvarige. Till exempel kan man hänvisa till Personuppgiftsbiträdesavtalets varaktighet.]

9. Övriga Instruktioner angående Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet

[Lägg vid behov till ytterligare Instruktioner för Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige utöver de som framgår ovan. Instruktionerna kan t.ex. avse förfarandet vid den Personuppgiftsansvariges granskningar och inspektioner av Personuppgiftsbiträdets Behandling av Personuppgifter enligt avsnitt 9 i PUB-avtalet.]