

## PERSONUPPGIFTSBITRÄDESAVTAL

Detta personuppgiftsbiträdesavtal har träffats mellan följande parter.

**Personuppgiftsansvarig:** \_\_\_\_\_

(Vårdgivarens namn, org.nr samt i förekommande fall ansvarig nämnd eller styrelse i landsting eller kommun)

**Personuppgiftsbiträde:** Mawell Scandinavia AB, org.nr 556432-3748.

### 1. Bakgrund och syfte

- 1.1 Behandling av personuppgifter ska utföras inom ramen för ett nationellt utvecklingsprojekt för e-förvaltningstjänster inom hälso- och sjukvården benämnd *Infektionsverktyget*. Syftet med Infektionsverktyget är att minska antalet vårdrelaterade och samhällsrelaterade infektioner inom hälso- och sjukvården genom bl.a. lokalt förbättringsarbete med stöd av patientuppgifter och jämförelsetal från medverkande vårdgivares verksamheter som sammanställs i Infektionsverktyget. Sambearbetade uppgifter ska återkopplas i pseudonymiserad form till den personuppgiftsansvarige. Personuppgifter från en vårdgivare får inte sambearbetas eller samköras med andra vårdgivares personuppgifter i Infektionsverktyget.
- 1.2 Personuppgiftslagen (1998:204) ställer krav på ett skriftligt avtal när ett personuppgiftsbiträde ska behandla personuppgifter för den personuppgiftsansvariges räkning. Detta avtal tecknas av den anledningen att personuppgiftsbiträdet saknar lagliga förutsättningar att på egen hand behandla *patientuppgifter*, dvs. personuppgifter om hälsa m.m.
- 1.3 Föreliggande avtal reglerar personuppgiftsbitrådets behandling av personuppgifter för den personuppgiftsansvariges vägnar på en fysisk datalagrings- och bearbetningsplats som förvaltas av personuppgiftsbiträdet. Personuppgiftsbitrådets åtagande omfattar samt är begränsat till de *personuppgifter och informationspaket* som framgår av [bilaga 1](#).
- 1.4 Avtalet omfattar all behandling av personuppgifter som personuppgiftsbiträdet utför för den personuppgiftsansvariges räkning på datalagrings- och bearbetningsplatsen. Syftet med avtalet är att se till att personuppgiftsbiträdet behandlar personuppgifterna i enlighet med den personuppgiftsansvariges *anvisningar* och i enlighet med tillämplig *lag, föreskrifter och praxis*. Avtalet syftar också till att reglera parternas skyldigheter och rättigheter i övrigt.

### 2. Begrepp och termer som används i avtalet

- 2.1 Med *personuppgiftsansvarig* avses den som är ansvarig för att behandlingen av personuppgifter är lagenlig samt bestämmer ändamålen med behandlingen och hur uppgifterna ska behandlas.

- 2.2 Med *personuppgiftsbiträde* avses den som behandlar personuppgifter för den personuppgiftsansvariges räkning.
- 2.3 Med *personuppgifter* avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet och som behandlas för den personuppgiftsansvariges räkning. Detta avtal gäller i förekommande fall även behandling av uppgifter om avlidna.
- 2.4 Med *registrerad* avses den som personuppgiften avser.
- 2.5 Med *behandling* avses varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, bevarande, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller rättelse.
- 2.6 Med *pseudonymisering* avses metoder som innebär att personuppgifter om enskilda inte ska kunna hänföras – direkt eller indirekt – till en fysisk individ. Det finns dock alltid en koppling till identiteten som kan återskapas när det behövs. Pseudonymisering är inte detsamma som avidentifiering, där kopplingen till person tas bort och aldrig kan återskapas. Pseudonymiserade uppgifter om enskilda är att betrakta som personuppgifter.

### 3. Personuppgiftsbitrådets åtaganden

#### *Allmänt*

- 3.1 Personuppgiftsbitrådet förbinder sig att följa patientdatalagen (2008:355) och personuppgiftslagen och samt hålla sig informerad om lagarna.
- 3.2 Personuppgiftsbitrådet och den eller de personer som arbetar under dennes ledning får endast behandla personuppgifter i enlighet med de *instruktioner* som anges i bilaga 2 eller som från tid till annan lämnas av den personuppgiftsansvarige eller behörig företrädare för denne. För det fall att personuppgiftsbitrådet saknar instruktioner som personuppgiftsbitrådet bedömer är nödvändiga för att genomföra uppdraget ska personuppgiftsbitrådet, utan dröjsmål, informera den personuppgiftsansvarige om sin inställning och invänta de instruktioner som den personuppgiftsansvarige bedömer erfordras.
- 3.3 Personuppgiftsbitrådet ska behandla personuppgifter på utrustning som fysiskt befinner sig i Sverige.
- 3.4 För det fall att registrerad, Datainspektionen eller annan tredje man begär information från personuppgiftsbitrådet som rör behandling av personuppgifter ska personuppgiftsbitrådet hänvisa till den personuppgiftsansvarige. Av punkten 3.2 ovan och punkten 5 nedan följer bland annat att personuppgiftsbitrådet inte får lämna ut personuppgifter eller annan information om behandlingen av personuppgifter utan skriftlig instruktion från den personuppgiftsansvarige.
- 3.5 Personuppgiftsbitrådet ska utan dröjsmål informera den personuppgiftsansvarige om eventuella kontakter från Datainspektionen eller Socialstyrelsen som rör eller kan vara av betydelse för behandling av personuppgifter. Personuppgiftsbitrådet har inte rätt att företräda den

personuppgiftsansvarige eller agera för den personuppgiftsansvariges räkning gentemot Datainspektionen, Socialstyrelsen eller annan tredje man.

#### *Säkerhetskrav*

3.6 Personuppgiftsbiträdet ska utöver vad som anges i bilaga 2 vidta skäligen tekniska, administrativa och organisatoriska åtgärder för att skydda personuppgifter mot obehörig åtkomst, förstörelse och ändring.

3.7 Den personuppgiftsansvarige har rätt att på egen bekostnad själv eller genom tredje man kontrollera att personuppgiftsbiträdet följer detta avtal. Personuppgiftsbiträdet ska därvid lämna den personuppgiftsansvariges representanter den assistans som behövs. Den personuppgiftsansvariges representanter ska ha rätt till inspektion av den hårdvara och mjukvara som används för behandling av personuppgifter som omfattas av detta avtal samt tillträde till de fysiska lokaler där utrustning och annan hård- och mjukvara finns.

3.8 Personuppgiftsbiträdet ska när detta avtal upphör att gälla överlämna personuppgifter/journaluppgifter på av den personuppgiftsansvarige angivet lagringsmedium och se till att det inte finns några personuppgifter kvar i egna system.

3.9 Personuppgiftsbiträdet ska assistera den personuppgiftsansvarige med att ta fram information som begärts av Datainspektionen eller registrerad. Den personuppgiftsansvarige ska ersätta personuppgiftsbiträdet för sådant arbete. Ersättningen ska avse personuppgiftsbitrådets självkostnader.

#### **4. Personuppgiftsansvariges åtaganden**

4.1 Den personuppgiftsansvarige ska se till att endast *personuppgifter och informationspaket* angivna i bilaga 1 utlämnas till Infektionsverket samt för de *ändamål* som anges i samma bilaga. Den personuppgiftsansvarige åtar sig vidare att se till att patientdatalagens och personuppgiftslagens bestämmelser efterlevs beträffande behandlingar av personuppgifter som innefattar både utlämnande av uppgifter till Infektionsverket samt efterföljande behandling av mottagna (pseudonymiserade) personuppgifter från verket.

4.2 Den personuppgiftsansvarige ska inom 30 dagar från avtalets tecknande presentera för personuppgiftsbiträdet interna rutiner och anvisningar för i *vilka fall och till vem* personuppgiftsbiträdet ska utlämna datafiler vilka innehåller information som möjliggör återskapande av registrerades identitet.

4.3 Den personuppgiftsansvarige ska vid elektroniskt utlämnande av uppgifter till Infektionsverket kryptera uppgifterna med en mellan parterna överenskommen krypteringsmetod, krypto eller krypteringsprodukt, oavsett om uppgifterna kommuniceras över Sjunet eller ett annat öppet nät.

4.4 Den personuppgiftsansvarige ansvarar bland annat för att *informera* registrerade om behandlingen, för att i nödvändiga fall inhämta *samttycke* från de registrerade och för att i tillämpliga fall *anmäla* behandlingar till Datainspektionen.

4.5 Den personuppgiftsansvarige ska utan dröjsmål informera personuppgiftsbiträdet om förändringar i behandlingen vilka påverkar personuppgiftsbitrådets skyldigheter. Den

personuppgiftsansvarige ska tillika informera personuppgiftsbiträdet om tredje parts, däribland Datainspektionens och registrerades åtgärder med anledning av behandlingen.

4.6 Den personuppgiftsansvarige ska hålla personuppgiftsbiträdet skadeslös för skador eller kostnader i anledning av behandlingen som är hänförliga till den personuppgiftsansvariges agerande. Personuppgiftsbiträdet ska snarast underrätta den personuppgiftsansvarige om anspråk på skadestånd som riktas mot biträdet med anledning av behandlingar av personuppgifter inom ramen för detta avtal.

## 5. Sekretess

Personuppgiftsbiträdet förbinder sig att inte till tredje man lämna ut eller eljest röja information om behandling av personuppgifter som omfattas av detta avtal eller annan information som personuppgiftsbiträdet erhållit till följd av detta avtal. Detta åtagande gäller inte information som personuppgiftsbiträdet föreläggs utge till Datainspektionen eller Socialstyrelsen.

Personuppgiftsbiträdet ska genast till den personuppgiftsansvarige överlämna en eventuell begäran från domstol, annan myndighet eller enskild om att få ta del av uppgifter som behandlas enligt detta avtal. Sekretessåtagandet gäller även efter att detta avtal i övrigt upphört att gälla. Personuppgiftsbiträdet åtar sig vidare att inte utnyttja personuppgifterna för egna ändamål.

## 6. Ersättning

Rätt till ersättning för behandling av personuppgifter i enlighet med detta avtal regleras i särskild ordning mellan den personuppgiftsansvarige och personuppgiftsbiträdet.

## 7. Ansvar mot tredje man

7.1 För den händelse registrerad, eller annan tredje man riktar krav mot den personuppgiftsansvarige på grund av personuppgiftsbiträdets behandling av personuppgifter ska personuppgiftsbiträdet hålla den personuppgiftsansvarige skadeslös för sådana krav som följer av att personuppgiftsbiträdet inte följt detta avtal. Den personuppgiftsansvarige ska skyndsamt informera personuppgiftsbiträdet om att sådant krav inkommit

7.2 För den händelse ett krav enligt punkt 7.1 avser personuppgifter eller informationspaket som inte framgår av bilaga 1, men som den personuppgiftsansvarige är ansvarig för att ha utlämnat till Infektionsverket, ska personuppgiftsbiträdet inte hållas skadeståndsansvarig. Motsvarande gäller för det fall att den personuppgiftsansvarige behandlar *personuppgifter* i Infektionsverket eller med hjälp av Infektionsverket för *ändamål* som inte framgår av bilaga 1.

## 8. Avtalstid

Avtalet gäller från dess undertecknande av båda parter och tills vidare. Avtalet upphör att gälla med omedelbar verkan om någon av parterna säger upp det. Personuppgiftsbiträdet ska då skyndsamt vidta åtgärder enligt 3.8 ovan.

## 9. Tvist

Tvist angående tolkning eller tillämpning av detta avtal ska avgöras av allmän domstol.

Detta avtal har upprättats i två exemplar, varav parterna har tagit ett vardera.

Ort och datum

---

För Mawell Scandinavia AB

---

(Underskrift)

---

(Namnförtydligande samt befattning)

För den personuppgiftsansvarige

---

(Underskrift)

---

(Namnförtydligande samt befattning)

## Personuppgifter, informationspaket samt ändamål som avses omfattas av personuppgiftsbiträdesavtalet mellan parterna

### 1. Ändamål för den personuppgiftsansvariges behandlingar i Infektionsverket

Den personuppgiftsansvariges behandling av personuppgifter i Infektionsverket sker i huvudsak för följande ändamål:

- a) Systematisk uppföljning och utvärdering av både vårdrelaterade och samhällsrelaterade infektioner i den personuppgiftsansvariges vård- respektive omsorgsverksamhet.
- b) Systematisk uppföljning och utvärdering av *profylaktisk antibiotikabehandling* i den personuppgiftsansvariges vård- respektive omsorgsverksamhet.
- c) Systematisk och fortlöpande utveckling och säkring av kvaliteten i den personuppgiftsansvariges vård- och omsorgsverksamhet (kvalitetssäkring) beträffande förebyggande av vårdrelaterade infektioner, t.ex. vid operationer och andra kirurgiska ingrepp, användning av urinavledande katetrar eller venösa katetrar, antibiotikabehandling, respiratorbehandling, behandling av *Clostridium Difficile* (antibiotikarelaterad diarré) m.m.
- d) Framställning av statistik (jämförelsetal) avseende a, b, och c.

Kommentar:

Med *utvärdering* avses i detta avtal analys och värdering av kvalitet, effektivitet och resultat av en verksamhet i förhållande till de mål som bestäms för denna. Med *uppföljning* avses fortlöpande och regelbunden mätning och beskrivning av den personuppgiftsansvariges behov, verksamheter och resursåtgången angivet i termer av t.ex. behovstäckning, produktivitet och nyckeltal. Uppföljningen tjänar till att ge en översiktlig bild av verksamhetens utveckling och att tjäna som en signal för avvikelser som bör beaktas.

Patientdatalagen förbjuder inte den personuppgiftsansvarige att använda *utlämnade* uppgifter från Infektionsverket för individuell vård eller behandling.

### 2. Relevanta och för ändamålen nödvändig information/personuppgifter

- a) Ordinationsorsak
  - i. Typ av antibiotika som ordinerats
  - ii. Ordinationstidpunkt
  - iii. Orsaken till ordinationen (typ av infektion/typ av profylaktisk behandling). Dessa kan specificeras på olika detaljeringsnivå.
  - iv. Ansvarig enhet
  - v. Patientens personuppgifter
    - a. Person-id
    - b. Kön
    - c. Födelsestidpunkt
- b) Laboratoriesvar
  - i. Förekomst av *Clostridium difficile*

- ii. Provtagningsstidpunkt
  - iii. Beställande enhet
  - iv. Patientens personuppgifter
    - a. Person-id
    - b. Kön
    - c. Födelsestidpunkt
- c) Patientplacering
- i. Placeringstid
  - ii. Enhet
  - iii. Patientens personuppgifter
    - a. Person-id
    - b. Kön
    - c. Födelsestidpunkt
- d) Aktiviteter (vilka aktiviteter som ska registreras bestäms lokalt)
- i. Typ av aktivitet
  - ii. Tid för utförande
  - iii. Utförande enhet
  - iv. Patientens personuppgifter
    - a. Person-id
    - b. Kön
    - c. Födelsestidpunkt
- e) Diagnoser
- i. Typ av diagnos
  - ii. Placeringstid
  - v. Enhet
  - vi. Patientens personuppgifter
    - a. Person-id
    - b. Kön
    - c. Födelsestidpunkt

## Informationssäkerhet

Personuppgiftsbiträdet åtar sig att arbeta systematiskt och fortlöpande med informationssäkerhet avseende behandlade personuppgifter i Infektionsverktyget enligt följande.

### Behörighet och åtkomstkontroll

1. Personuppgiftsbiträdet ska ansvara för att det finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter för åtkomst till Infektionsverktyget.
2. Autentisering till Infektionsverktyget ska bygga på två faktorer (tvåfaktorsautentisering).
3. Personuppgiftsbiträdet ska ha rutiner som säkerställer att
  - a. det av dokumentationen av åtkomsten (loggarna) framgår vilka åtgärder som har vidtagits med uppgifterna i Infektionsverktyget,
  - b. det av loggarna framgår vem och vid vilken tidpunkt åtgärderna har vidtagits,
  - c. användarens och patientens identitet framgår av loggarna,
  - d. systematiska och återkommande stickprovskontroller av loggarna görs,
  - e. genomförda kontroller av loggarna dokumenteras, och
  - f. loggarna får gallras först tio år efter loggningstillfället.Om någon av parterna säger upp avtalet ska personuppgiftsbiträdet utlämna loggarna till den personuppgiftsansvarige.

### Säkerhetskopiering av Infektionsverktyget

4. Personuppgiftsbiträdet ska ha rutiner för säkerhetskopiering av personuppgifter. Av rutinerna ska det framgå
  - a. att säkerhetskopiering av den personuppgiftsansvariges uppgifter i Infektionsverktyget ska göras dagligen,
  - b. att säkerhetskopiorna ska sparas tre månader, och
  - c. att återläsningstester ska göras en gång i månaden.Om någon av parterna säger upp avtalet ska personuppgiftsbiträdet utlämna säkerhetskopiorna till den personuppgiftsansvarige.
5. Personuppgiftsbiträdet ska ansvara för att säkerhetskopior förvaras på ett betryggande sätt och väl åtskilda från originaluppgifterna.
6. Personuppgiftsbiträdet ska i övrigt skydda den personuppgiftsansvariges uppgifter i Infektionsverktyget mot obehörig åtkomst, förstörelse eller ändring.

### Pseudonymisering

7. Personuppgiftsbiträdet ska vid sambearbetning av personuppgifter i Infektionsverktyget respektive utlämnande av personuppgifter till den personuppgiftsansvarige *pseudonymisera* behandlade personuppgifter (se definition i punkt 2 i avtalet). Datafiler vilka innehåller information om kopplingen mellan individ och personsättningsnummer eller kryptonyckel ska förvaras på ett betryggande sätt av personuppgiftsbiträdet och utan insyn för obehöriga. Personuppgiftsbiträdet ska utlämna datafiler som möjliggör

återskapande av registrerades identitet till den personuppgiftsansvarige på dennes begäran, om utlämnandet är förenligt med de rutiner och anvisningar som den personuppgiftsansvarige enligt punkten 4.2 i avtalet ska dokumentera och presentera för personuppgiftsbiträdet.

### **Informationsöverföring**

8. Personuppgiftsbiträdet ska vid elektroniskt utlämnande av uppgifter från Infektionsverktyget till personuppgiftsansvarig kryptera uppgifterna med mellan parterna överenskommen krypteringsmetod, krypto eller krypteringsprodukt, oavsett om uppgifterna kommuniceras över Sjunet eller ett annat öppet nät.
9. Ingen form av överföring av information som regleras i detta avtal får äga rum utan att erforderliga tekniska specifikationer rörande överföringssätt m.m. upprättats, utväxlats och godkänts av utsedda och ansvariga kontaktpersoner hos respektive part. Överföring får heller aldrig ske i strid med de tekniska specifikationer som fastställts mellan parterna. Inte heller får överföring ske om sättet som överföring sker på förändras och utsedda kontaktpersoner inte har godkänt denna förändring.
10. Innan personuppgiftsbiträdet driftsätter sina system för mottagande eller utlämnande av information enligt detta avtal ska systemen kvalitetssäkras genom tester. Den personuppgiftsansvarige ska godkänna personuppgiftsbitrådets genomförda tester innan skarp drift får påbörjas.
11. När systemet och informationsöverföringen mellan den personuppgiftsansvarige och Infektionsverktyget är i drift ska parterna genom tester och övervakning löpande kontrollera säkerheten och kvaliteten i systemet enligt respektive parts dokumenterade rutiner.
12. Om personuppgiftsbiträdet avser att göra förändringar i sitt system (uppgradering, patchning etc.) på sätt som kan förväntas påverka informationsöverföringen ska bitrådets kontaktperson i projektet underrätta den personuppgiftsansvariges kontaktperson om detta och inhämta godkännande. Sådant samråd ska ske i så god tid att parterna gemensamt kan genomföra erforderliga tester för att säkerställa normal drift efter genomförda förändringar. Samråden skall dokumenteras och resultera i en dokumenterad plan för testning och driftsättning.
13. Driftstörningar hos personuppgiftsbiträdet som påverkar informationsöverföringen mellan parterna negativt ska omedelbart vid upptäckt anmälas till den andra parten. Vid driftstörningar eller underhåll som kan påverka informationsöverföringen mellan parterna negativt och som kan beräknas vara längre än 24 timmar ska personuppgiftsbiträdet ha förberedda alternativa lösningar för informationsöverföring.
14. Intrångsförsök eller annat bedrägligt förfarande för att få åtkomst till den personuppgiftsansvariges uppgifter i Infektionsverktyget ska omedelbart anmälas av personuppgiftsbiträdet vid upptäckt till den andra parten. Inga ändringar (omstart, uppgraderingar, felsökningar) får normalt vidtas utan samråd med den andra parten.
15. Den personuppgiftsansvarige ansvarar för förlust, försening, förvanskning och/eller obehörigt intrång i datafiler efter det att de lämnat användarapplikationen till dess att den

är mottagen av personuppgiftsbiträdets system. Båda parterna ansvarar vidare för att datafilerna krypteras enligt överenskommelse mellan parterna. Personuppgiftsbiträdet ansvarar för förlust, försening, förvanskning och/eller obehörigt intrång i datafilerna efter att den har mottagits av personuppgiftsbiträdets system.

16. Personuppgiftsbiträdet åtar sig att kontinuerligt logga systemhändelser och kommunikation enligt detta avtal. System- och säkerhetsloggar skall ha ett adekvat säkerhetsskydd. Loggar får gallras först ett år efter loggningstillfälle.