

## DATABESKYTTELSAFTALE TEKNISK SUPPORT OG VEDLIGEHOLDELSE

*Denne databeskyttelsesaftale og dens bilag ("DBA") fastsætter minimumsstandarder for databeskyttelse og cybersikkerhed og relaterede krav og udgør en del af kontrakten, herunder en handelsaftale, en serviceaftale eller en ordre ("Aftalen") (undtagen Cepheid C360-brugeraftalen). Denne databeskyttelsesaftale indgås af og mellem Kunden (som defineret i aftalen) og Cepheid (som defineret i aftalen) og skal forblive fuldt ud gældende i Aftalens gyldighedsperiode. Cepheid og Kunden omtales i det følgende hver for sig som en "Part" eller kollektivt som "Parterne".*

*Parterne er enige om, at hvis der sker behandling af personoplysninger i henhold til Aftalen, gælder vilkårene i denne databeskyttelsesaftale for den pågældende Aftale, uanset om der udtrykkeligt henvises til den pågældende Aftale eller ej.*

DERFOR, under hensyntagen til de præmisser der er anført ovenfor, og de heri indeholdte gensidige aftaler, er parterne enige om følgende:

### 1. Definitioner.

- (A) "Gældende lov" betyder enhver lov (herunder alle verdensomspændende love og bestemmelser om databeskyttelse og privatlivets fred, der gælder for de pågældende personoplysninger, herunder, hvor det er relevant, EU's databeskyttelseslovgivning eller POPIA), regel eller bestemmelse, der gælder for Aftalen, tjenesterne eller parterne, og gældende industristandarder vedrørende privatlivets fred, databeskyttelse, fortrolighed, informationssikkerhed, tilgængelighed og integritet eller håndtering eller behandling (herunder opbevaring og videregivelse) af personoplysninger, som kan blive ændret, reguleret, omformuleret eller erstattet fra tid til anden.
- (B) "dataansvarlig", "databehandler", "registreret", "personoplysninger eller personlige oplysninger", "behandling", "behandling", "særlige kategorier af personoplysninger" og "følsomme personoplysninger" har den betydning, der er angivet i gældende lovgivning.
- (C) "Databrud" betyder (i) tab eller misbrug (uanset hvordan) af personoplysninger, (ii) utilsigtet, uautoriseret og/eller ulovlig videregivelse, adgang, ændring, korruption, overførsel, salg, udlejning, destruktion eller brug af personoplysninger, (iii) enhver anden handling eller undladelse, der kompromitterer eller kan kompromittere sikkerheden, fortroligheden eller integriteten af personoplysninger, eller (iv) ethvert brud på sikkerhedsforanstaltningerne.
- (D) "EU / britisk / schweizisk databeskyttelseslovgivning" betyder (i) Europa-Parlamentets og Rådets forordning 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (den generelle databeskyttelsesforordning ("EU GDPR")); (ii) EU GDPR, som den er indarbejdet i Storbritanniens lovgivning i henhold til afsnit 3 i Storbritanniens lov om Den Europæiske Union (tilbagetrækning) 2018 ("UK GDPR"); (iii) i Schweiz den føderale lov om databeskyttelse af 19. juni 1992 (revideret udgave) ("FADP"); (iv) EU's e-databeskyttelsesdirektivet (direktiv 2002/58/EF); og (iv) alle gældende nationale databeskyttelseslove, der er udstedt i henhold til eller i medfør af (i), (ii) eller (iii); i hvert enkelt tilfælde som ændret eller erstattet fra tid til anden.

- (E) "Personoplysninger" betyder, i enhver form, format eller medie, enhver (a) fortrolig information om Kunden og/eller (b) data, dvs. enhver information, der kan identificere en person. For klarhedens skyld betyder persondata også personoplysninger.
- (F) "POPIA" betyder Loven om beskyttelse af personlige oplysninger, Sydafrika, en lov, der omhandler beskyttelse og regulering af behandling af personlige oplysninger i Republikken Sydafrika, som blev godkendt den 13. november 2013 og trådte i kraft den 1. juli 2020.
- (G) "Begrænset overførsel" betyder (i) hvor EU's GDPR finder anvendelse, en overførsel af personoplysninger til et land uden for Det Europæiske Økonomiske Samarbejdsområde, som ikke er underlagt en fastsættelse af tilstrækkelig beskyttelse fra Europa-Kommissionen; (ii) hvor UK GDPR gælder, en overførsel af personoplysninger til ethvert andet land, som ikke er baseret på forordninger om tilstrækkelig beskyttelse i henhold til afsnit 17A i Storbritanniens lov om databeskyttelse 2018; (iii) hvor FADP finder anvendelse, en grænseoverskridende offentliggørelse i mangel af lovgivning, der garanterer tilstrækkelig beskyttelse i henhold til artikel 6 i FADP og (iv) hvor POPIA finder anvendelse, en grænseoverskridende overførsel, videregivelse eller udveksling af oplysninger uden for Republikken Sydafrika.
- (H) "Standardkontraktbestemmelser" betyder (i) hvor EU's GDPR finder anvendelse, de kontraktbestemmelser, der er knyttet til Europa-Kommissionens gennemførelsesafgørelse 2021/914 af 4. juni 2021 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til forordning (EU) Europa-Parlamentet og Rådet 2016/679 ("EU standardkontraktbestemmelser«); (ii) hvor UK GDPR finder anvendelse, "Tillæg om international dataoverførsel til EU-Kommissionens standardkontraktbestemmelser" udstedt af Informationskommissæren i henhold til s.119A(1) i Data Protection Act 2018 ("Tillæg for Storbritannien"); (iii) hvor FADP finder anvendelse, de modelkontrakter og standardkontraktbestemmelser, der er anerkendt af den schweiziske føderale databeskyttelses- og informationskommissær ("FDPIC") i henhold til artikel 6, stk. 2, litra a, i FADP i overensstemmelse med erklæringen fra FDPIC af 27. august 2021 (oprindeligt tilgængelig på <https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2021/Paper%20SCC%20def.en%2024082021.pdf.download.pdf/Paper%20SCC%20def.en%2024082021.pdf>) ("Tillæg for Schweiz"); og (iv) hvor POPIA anvender kontraktbestemmelser relateret til beskyttelse, behandling og overførsel af personoplysninger udført af to eller parter i relation til sådanne oplysninger.
- (I) "Tjenester" betyder de tjenester, som Cepheid udfører i henhold til Aftalen.
- (J) "Underdatabehandler": enhver enhed eller person, som Databehandleren udliciterer sit ansvar til.
- (K) Hvis det er relevant, andre udtryk med store bogstaver som defineret i Aftalen.

## 2. Parternes indbyrdes forhold:

2.1 Kunden (den "dataansvarlige") udpeger Cepheid som databehandler til at behandle de personoplysninger, der er beskrevet i bilag 1 til denne databeskyttelsesaftale, til de formål, der er beskrevet deri (eller som parterne på anden måde skriftligt har aftalt) ("det tilladte formål"). Hver part skal overholde de forpligtelser, der gælder for den i henhold til gældende lovgivning.

Kunden anerkender og accepterer, at Cepheid kan anvende sine datterselskaber og/eller tredjeparts underdatabehandlere i forbindelse med levering af tjenesterne. Cepheid forbliver fuldt ud ansvarlig over for Kunden for en sådan tredjepart og indgår en skriftlig og eksigibel aftale med en sådan

tredjepart, der indeholder vilkår, som ikke er mindre restriktive end de forpligtelser, der gælder for Kunden i henhold til denne databeskyttelsesaftale.

2.2 Cepheid indsamler og behandler de nødvendige identifikationsdata med henblik på indgåelse og udførelse af Aftalen, og mere generelt til forvaltningen af Parternes forretningsforbindelser, for at sende information om produkter, varer og tjenester eller relaterede produkter, varer eller tjenester fra datterselskaber .

Yderligere oplysninger om Cepheid's privatlivspolitik kan fås på Cepheid's hjemmeside eller ved at kontakte Cepheid på e-mailadressen: [privacy.officer@cepheid.com](mailto:privacy.officer@cepheid.com)

Kunden forpligter sig til at informere enhver berørt registreret om Cepheid's behandlingsaktiviteter og videregive Cepheid's fortrolighedserklæring i overensstemmelse hermed.

### 3. Generelle krav.

3.1 Når Cepheid behandler personoplysninger på vegne af Kunden, skal Cepheid:

- i) overholde alle gældende love, herunder gældende lov, når der behandles personoplysninger;
- ii) medmindre det kræves i henhold til gældende lovgivning, kun behandle personoplysninger på vegne af Kunden og kun i det omfang, det er nødvendigt for at levere tjenesterne til Kunden og i overensstemmelse med alle gældende love, herunder gældende lovgivning, og Kundens dokumenterede instruktioner;
- iii) implementere og vedligeholde passende og rimelige tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der er passende i forhold til risikoen, herunder, hvor det er relevant, de foranstaltninger, der er omhandlet i artikel 32, stk. 1, i EU's og Storbritanniens GDPR (herunder kravene til PCI-DSS betalingskortindustriens datasikkerhedsstandard, hvis Cepheid behandler kortindehaver- eller andre finansielle kontooplysninger) for at beskytte personoplysningerne (i) mod utilsigtet eller ulovlig tilintetgørelse og (ii) mod tab, ændring, uautoriseret videregivelse af eller adgang til personoplysningerne; sådanne foranstaltninger skal som minimum omfatte de foranstaltninger, der er identificeret i bilag 2;
- iv) kun tillade adgang til personoplysninger til Cepheid-personale, der har brug for adgang til de relevante personoplysninger i det omfang, det er rimeligt nødvendigt for Aftalens formål, idet alle sådanne personer er underlagt en tavshedspligt;
- v) yde al rimelig og rettidig bistand (herunder ved at implementere passende og rimelige tekniske og organisatoriske foranstaltninger) for at hjælpe Kunden med at reagere på: (i) enhver anmodning fra en Registreret om at udøve sine rettigheder i henhold til gældende lov (herunder retten til adgang, rettelser, indsigelse, sletning og dataportabilitet, alt efter hvad der er relevant); og (ii) enhver anden korrespondance, forespørgsel eller klage modtaget fra en Registreret, tilsynsmyndighed eller anden tredjepart i forbindelse med behandlingen af personoplysningerne. Hvis en sådan anmodning, korrespondance, forespørgsel eller klage fremsættes direkte til Cepheid, skal Cepheid straks informere Kunden herom og give alle detaljer om det samme;
- vi) straks underrette Kunden om:
  - a) enhver anmodning, forespørgsel, klage, meddelelse eller kommunikation modtaget fra en tredjepart, herunder en Registreret eller en tilsynsmyndighed, med hensyn til

personoplysninger og overholde instruktionerne fra Kunden i forbindelse med besvarelse af en sådan anmodning, forespørgsel, klage, meddelelse eller kommunikation; og

- b) enhver instruks fra Kunden, som Cepheid mener er i strid med gældende lovgivning, herunder gældende lovgivning;
- vii) i tilfælde af international overførsel er parterne enige om, at når overførslen af personoplysninger er en begrænset overførsel, skal den være omfattet af de relevante standardkontraktbestemmelser som anført i bilag 3.
- viii) på Kundens rimelige anmodning og med rimeligt varsel indsende de faciliteter, som den anvender til behandling af personoplysninger og/eller personoplysningerne, til revision, som skal udføres af repræsentanter for Kunden eller et revisionsorgan, som begge parter er enige om, idet omkostningerne forbundet hermed udelukkende bæres af Kunden;
- ix) føre passende optegnelser, der understøtter dens overholdelse af dens forpligtelser i henhold til denne databeskyttelsesaftale, og stille dem til rådighed for Kunden i forbindelse med enhver revision, der er nævnt i (viii) ovenfor;
- x) ikke overføre personoplysninger fra en jurisdiktion til en anden jurisdiktion, uden Kundens forudgående skriftlige samtykke, medmindre Cepheid har indført standardkontraktklausuler i forbindelse med begrænset overførsel af personoplysninger;
- xi) med rimelighed bistå og samarbejde med Kunden, herunder bistå Kunden med en konsekvensanalyse af databeskyttelse eller en konsekvensanalyse af privatlivets fred (som krævet i henhold til gældende lovgivning) og forudgående konsultationer med de relevante myndigheder, for at bistå Kunden med at overholde sine forpligtelser i henhold til gældende lovgivning;
- xii) kun opbevare personoplysningerne så længe det er nødvendigt for at udføre tjenesterne, og ved afslutningen af leveringen af tjenesterne efter Kundens valg slette eller returnere personoplysningerne til Kunden (medmindre andet udtrykkeligt kræves i henhold til gældende lovgivning) og på anmodning give Kunden en skriftlig bekræftelse på, at dette afsnit er overholdt;
- xiii) hvis Cepheid med rimelighed har mistanke om eller bliver opmærksom på et databrud:
  - a) give Kunden skriftlig meddelelse om samme uden unødigt forsinkelse og under ingen omstændigheder senere end fireogtyve (24) timer efter at have fået kendskab til et sådant formodet eller bekræftet databrud;
  - b) give Kunden oplysninger så Kunden har mulighed for at rapportere eller informere de registrerede om databruddet efter behov;
  - c) foretage en undersøgelse af et sådant databrud og samarbejde med Kunden, tilsynsmyndigheder og retshåndhævende myndigheder på en rimelig måde;
  - d) ikke udsende nogen offentlige meddelelser vedrørende et sådant databrud uden Kundens forudgående skriftlige godkendelse, som ikke skal tilbageholdes urimeligt; og
  - e) træffe rimelige korrigerende foranstaltninger i tide for at bistå med efterforskning, begrænsning og afhjælpning af et databrud, for at afhjælpe og mindske risikoen for gentagelse af et sådant databrud, og

xiv) underkaste sig det valg af jurisdiktion, der er fastsat i Aftalen, med hensyn til enhver tvist eller ethvert krav, der måtte opstå i forbindelse med denne databeskyttelsesaftale, herunder tvister vedrørende dens eksistens, gyldighed eller ophør eller konsekvenserne af dens ugyldighed; og denne databeskyttelsesaftale og alle forpligtelser uden for kontraktforhold eller andre forpligtelser, der opstår i forbindelse med den, er underlagt lovgivningen i det land eller område, der er fastsat til dette formål i Aftalen.

3.2 Parterne må ikke deltage i (eller tillade, at en underdatabehandler deltager i) andre begrænsede overførsler af personoplysninger (uanset om det er som eksportør eller importør af personoplysningerne), medmindre den begrænsede overførsel sker i fuld overensstemmelse med gældende lovgivning og i henhold til standardkontraktbestemmelser, der er implementeret mellem den relevante eksportør og importør af personoplysningerne.

3.3 Kunden bemyndiger Cepheid til at udpege underdatabehandlere (og tillader hver enkelt underdatabehandler, der er udpeget, at udpege andre databehandlere) i overensstemmelse med afsnit 3.3 og eventuelle begrænsninger i Aftalen.

3.3.1 Kunden giver hermed et generelt samtykke til, at Cepheid kan anvende underdatabehandlere, der allerede er ansat på datoen for denne databeskyttelsesaftale, forudsat at Cepheid fortsat er fuldt ud ansvarlig over for Kunden for en sådan tredjepart og i hvert enkelt tilfælde så hurtigt som muligt indgår en skriftlig og gennemførlig aftale med en sådan tredjepart, der indeholder vilkår, som ikke er mindre restriktive end de forpligtelser, der gælder for Cepheid i henhold til denne databeskyttelsesaftale.

3.3.2 Cepheid opretholder en liste over sine autoriserede underdatabehandlere, som kan fås efter anmodning.

#### 4. Diverse.

Hvis det er relevant, er det standardkontraktbestemmelserne, herunder bilag 1-4, der gælder og har forrang i tilfælde af konflikt eller uoverensstemmelse mellem vilkårene i denne databeskyttelsesaftale og standardkontraktbestemmelserne.

## Bilag 1 Beskrivelse af databehandling

Dette bilag 1 udgør en del af databeskyttelsesforordningen og beskriver den behandling, som databehandleren vil udføre på vegne af den dataansvarlige.

### Liste over parter

#### Databehandler:

1.	Navn:	Cepheid, enhed identificeret i Aftalen
	Adresse:	Som defineret i Aftalen
	Kontaktpersonens navn, stilling og kontaktoplysninger:	Som defineret i Aftalen eller mellem Parterne
	Aktiviteter, der er relevante for de data, der overføres i henhold til disse bestemmelser:	Beskrevet i dette bilag 1
	Rolle:	Databehandler

#### Dataansvarlig:

1.	Navn:	Kunde, enhed identificeret i Aftalen
	Adresse:	Som defineret i Aftalen
	Kontaktpersonens navn, stilling og kontaktoplysninger:	Som defineret i Aftalen eller mellem Parterne
	Aktiviteter, der er relevante for de data, der overføres i henhold til disse bestemmelser:	Beskrevet i dette bilag 1
	Rolle:	Dataansvarlig

### Beskrivelse af overførslen

#### Genstand for behandlingen

Personoplysninger behandles til følgende formål:

Teknisk support, optimering af arbejdsgange, support på højt niveau, minimere nedetid for Kunden, reagere på feedback fra Kunden, regulatoriske spørgsmål, måling, kundeanalyser, verifikation af tilslutningsmuligheder (fejlfinding, implementering / LIS (laboratorieinformationssystem)), overvågning efter markedsføring, eller revisionsformål.

#### Behandlingens varighed

Personoplysninger vil blive behandlet indtil:

Kundeanalyse: Behandles så længe det er nødvendigt for at opfylde formålene og levere de ønskede tjenester i henhold til Aftalen, medmindre andet er skriftligt aftalt

Teknisk support, support på højt niveau, minimere nedetid for Kunden, reagere på feedback fra Kunden, regulatoriske spørgsmål, måling, kontrol af tilslutningsmuligheder: indtil problemet er løst

Alle data kan opbevares i arkiver med henblik på overvågning efter markedsføring eller revisionsformål i en opbevaringsperiode afhængigt af forordningen

#### Overførselsfrekvens

Personoplysningerne vil blive behandlet løbende.

**Behandlingens art:**

**Behandlingsaktiviteter**

Personoplysningerne vil blive underlagt følgende grundlæggende behandlingsaktiviteter:

Registrering, opbevaring, konsultation, brug, videregivelse ved overførsel, kombination, begrænsning, sletning eller destruktions, anonymisering, pseudonymisering og som fastsat i Aftalen.

**Kategorier af registrerede**

De personoplysninger, der skal behandles, vedrører følgende kategorier af registrerede:

Patienter hos Kunden

Kunden og dennes ansatte

**Kategorier af personoplysninger**

De personoplysninger, der skal behandles, vedrører følgende datakategorier:

Afhængigt af de data, som Kunden har indtastet i instrumentkonsollen og/eller modtaget af laboratorieinformationssystemet, kan følgende data behandles til de forskellige formål, der er anført ovenfor: Prøve-ID, telemetri-data fra instrumentet (temperatur, spændinger, tryk, systemadvarsler og alarmer), testresultater, navn, efternavn, patient-ID (data kan omfatte følsomme eller særlige kategorier af personoplysninger)

**Kompetent myndighed**

Dette vil være tilsynsmyndigheden i den EU-medlemsstat, hvor eksportøren er etableret, Information Commission, hvis eksportøren er etableret i Storbritannien ("UK"), eller FDPIC, hvis eksportøren er etableret i Schweiz. Hvis eksportøren ikke er etableret i en EU-medlemsstat, Storbritannien eller Schweiz, men er omfattet af EU's/Storbritanniens/schweiziske databeskyttelseslovgivning, vil dette være tilsynsmyndigheden i den jurisdiktion, hvor Cepheids repræsentant er etableret (som krævet i henhold til EU's/Storbritanniens/schweiziske databeskyttelseslovgivning). Hvis udpegelse af en repræsentant ikke er påkrævet i henhold til EU's/Storbritanniens/schweizisk databeskyttelseslovgivning, vil tilsynsmyndigheden være CNIL i Frankrig, hvis de personer, hvis oplysninger overføres, befinder sig i EU, Information Commissioner, hvis de fysiske personer befinder sig i Storbritannien, eller FDPIC, hvis de fysiske personer befinder sig i Schweiz. Hvis personoplysningerne stammer fra Canada, vil tilsynsmyndigheden være en af de kommissærer, der har jurisdiktion over sagen som fastsat i den gældende databeskyttelseslovgivning.

## Bilag 2

### Beskrivelse af de tekniske og organisatoriske foranstaltninger, som Cepheid har implementeret

Dette bilag 2 udgør en del af databeskyttelsesaftalen og beskriver de tekniske og organisatoriske foranstaltninger, som Cepheid har implementeret i overensstemmelse med artikel 32(1) i GDPR og andre gældende databeskyttelseslove.

#### 1- På lokaliteten:

Cepheid-medarbejdere kan bruge et krypteret USB-drev til at udtrække nødvendige kundeinstrumentdata til at afhjælpe tekniske problemer og instrumentydelse.

I forbindelse med besøg til fastlæggelse af optimering af ydelse har Cepheid-medarbejdere kun adgang til de mindst nødvendige data, som ikke indeholder nogen af patientens sundhedsoplysninger. Dataene overføres til medarbejderens notebook, behandles med henblik på generering af kunderapporter med anbefalinger og slettes derefter i henhold til Standard Work og Cepheid politik for opbevaring af data.

#### 2- Fjernbetjening:

Adgangsrolle: Kun medarbejdere i Cepheid teknisk support og område support har sikret adgang til instrumenterne.

Til fjernsupport til håndtering af klager kan Cepheid-agenter bruge RDS-sessioner (Remote Desktop Sharing), men kun efter at sessionen er godkendt af Kunden i hvert tilfælde.

Dataoverførsel: I henhold til Cepheid-politik overføres data via en sikker krypteret metode til interne Cepheid-servere, så tilknyttede personer kan deltage i kundesupportaktiviteter (der anvendes TLS 1.2+-protokoller til sikrede transaktioner).

#### 3- Kunden sender data:

Afsendelse pr. e-mail, på hjemmesideplatform eller pr. fax: data sendes af Kunden via en sikker krypteret metode til en intern Cepheid-medarbejder inden for regionen. Som dataansvarlig er Kunden ansvarlig for at anonymisere personoplysninger og kun uploade det minimum af data, der kræves, før de overføres til Cepheid (Cepheid-instrumentsoftware giver Kunden mulighed for at sløre specifikke personoplysninger og sundhedsdata i sin instrumentrapport før eksport).

#### 4- Dataoverførsler inden for Cepheid Support-funktioner:

Hvis der er behov for yderligere support uden for Kundens hjemområde, vil alene de nødvendige oplysninger blive overført; unødvendige personoplysninger og sundhedsdata vil blive slettet/anonymiseret, hvor det er muligt\*, og dataene vil blive sendt via en sikker delingsmetode. Data i hvile er krypteret og destrueres i henhold til Cepheid's relevante politik for kundeservice.

#### 5- Politik og praksis:

Cepheid sikrer løbende fortrolighed, integritet, tilgængelighed og modstandsdygtighed af behandlingssystemer og tjenester. Med henblik herpå har de mulighed for rettidigt at genoprette tilgængeligheden af og adgangen til relevante data om servicesupport og klagesagsbehandling i Cepheids systemer i tilfælde af en fysisk eller teknisk hændelse.

#### 6- Processer:

Cepheid har en proces til regelmæssigt at teste, vurdere og evaluere effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden.

\* Proceduren for afidentificering/anonymisering er instrumentspecifik.



### **Bilag 3**

#### **Overførselsbestemmelser i Storbritannien, EU og Schweiz**

Dette bilag 3 udgør en del af databeskyttelsesaftalen og angiver, hvordan standardkontraktbestemmelserne (SCC) skal udfyldes:

1. Hvis EU standardkontraktbestemmelserne anses for at være indgået og inkorporeret i denne databeskyttelsesaftale ved henvisning mellem parterne, vil EU standardkontraktbestemmelserne blive udfyldt på følgende måde:
  - (i) Modul 2 finder anvendelse i det omfang, Kunden er dataansvarlig for personoplysningerne;
  - (ii) i punkt 7 vil den valgfrie docking-bestemmelse være gældende;
  - (iii) i punkt 9, gælder valgmulighed 2, og fristen for forudgående meddelelse om ændringer af underdatabehandlere skal være som fastsat i punkt 3.2 i denne databeskyttelsesaftale;
  - (iv) i punkt 11, finder det valgfrie sprog ikke anvendelse;
  - (v) i punkt 17, finder valgmulighed 2 anvendelse, og EU standardkontraktbestemmelserne er underlagt loven i den jurisdiktion, hvor dataeksportøren er etableret, hvor det er relevant, og hvor en sådan lov giver mulighed for tredjemands rettigheder, og ellers fransk lov;
  - (vi) i punkt 18, litra b), skal tvister afgøres ved domstolene i dataeksportørens land og ellers ved domstolene i Frankrig;
  - (vii) Bilag I til EU's standardkontraktbestemmelser anses for at være udfyldt;
    - (A) Del A: med de oplysninger, der er anført i bilag 1 til denne databeskyttelsesaftale;
    - (B) Del B: med den relevante beskrivelse af behandlingen, der er anført i bilag 1 til denne databeskyttelsesaftale, og
    - (C) Del C: i overensstemmelse med kriterierne i punkt 13, litra a), i EU's standardkontraktbestemmelser;
  - (viii) Bilag II: med minimumssikkerhedsforanstaltningerne, og
2. Hvis tillægget for Storbritannien anses for at være indgået og inkorporeret i denne databeskyttelsesaftale ved henvisning mellem parterne, vil tillægget for Storbritannien blive udfyldt på følgende måde:
  - a. EU's standardkontraktbestemmelser der er udfyldt som anført ovenfor i punkt 1 i dette bilag 3, finder også anvendelse på overførsler af sådanne personoplysninger, jf. dog underpunkt 2.b i dette bilag 3 nedenfor;

- b. Tabel 1 til 3 i tillægget for Storbritannien anses for at være udfyldt med de relevante oplysninger fra EU's standardkontraktbestemmelser, udfyldt som anført ovenfor, og i tabel 4 anses "ingen af parterne" for at være afkrydset. Startdatoen for tillægget for Storbritannien (som anført i tabel 1) er ikrafttrædelsesdatoen.
3. Hvis tillægget for Schweiz anses for at være indgået og inkorporeret i denne databeskyttelsesaftale ved henvisning mellem parterne, vil tillægget for Schweiz blive udfyldt på følgende måde:
  - a. EU's standardkontraktbestemmelser der er udfyldt som anført ovenfor i punkt 1 i dette bilag 3, finder også anvendelse på overførsler af sådanne personoplysninger, jf. dog underpunkt 3.b i dette bilag 3 nedenfor;
  - b. de Standardkontraktbestemmelser, der er indarbejdet ved henvisning, skal beskytte personoplysninger om juridiske enheder i Schweiz indtil ikrafttrædelsen af den reviderede FADP.
4. Hvis hverken underpunkt 1, underpunkt 2 eller underpunkt 3 i dette bilag 3 finder anvendelse, samarbejder parterne i god tro om at gennemføre passende sikkerhedsforanstaltninger for overførsel af sådanne personoplysninger som krævet eller tilladt i henhold til den gældende lovgivning uden unødigt forsinkelse.

## Bilag 4

### 4.1 Supplerende krav til overførsel af personoplysninger ud af Det Europæiske Økonomiske Samarbejdsområde

Følgende supplerende krav gælder for alle begrænsede overførsler:

1. Kunden skal regelmæssigt stille oplysninger til rådighed for Cepheid om offentlige myndigheders anmodninger om adgang til personoplysninger og den måde, hvorpå der gives svar (hvis det er tilladt i henhold til lovgivningen);
2. Kunden garanterer, at den ikke med overlæg har oprettet tekniske bagdøre eller interne processer for at lette offentlige myndigheders direkte adgang til personoplysninger, og at den ikke i henhold til gældende lovgivning eller praksis er forpligtet til at oprette eller vedligeholde bagdøre;
3. Kunden skal forespørge enhver offentlig myndighed, der fremsætter en anmodning om adgang til personoplysninger, om den samarbejder med andre statslige myndigheder i forbindelse med sagen;
4. Kunden skal yde rimelig bistand til registrerede personer i forbindelse med udøvelsen af deres rettigheder til personoplysninger i den modtagende jurisdiktion;
5. Kunden skal samarbejde med Cepheid i tilfælde af, at en relevant tilsynsmyndighed eller domstol beslutter, at en overførsel af personoplysninger skal være underlagt specifikke yderligere sikkerhedsforanstaltninger;
6. Kunden skal implementere kryptering og/eller andre tekniske foranstaltninger, der er tilstrækkelige til at yde rimelig beskyttelse mod offentlige myndigheders opfangning af personoplysninger under transit eller anden uautoriseret adgang; og
7. Kunden skal have passende politikker og procedurer på plads, herunder uddannelse, således at anmodninger om adgang til personoplysninger fra offentlige myndigheder videresendes til den relevante funktion og håndteres korrekt.

### 4.2 Supplerende krav til overførsel af personoplysninger ud af Republikken Sydafrika

Følgende supplerende krav gælder for overførsel af personoplysninger ud af Republikken Sydafrika:

1. Overførsel af personoplysninger uden for Sydafrika skal opfylde følgende parametre:
  - (A) den Part, der er modtageren af oplysningerne, er underlagt en lov, bindende virksomhedsregler eller bindende aftale, der giver et tilstrækkeligt beskyttelsesniveau, som:
    1. effektivt opretholder principper for rimelig behandling af oplysningerne, der i alt væsentligt svarer til betingelserne for lovlig behandling af personoplysninger vedrørende en registreret, som er en fysisk [person](#) og, hvor det er relevant, en juridisk [person](#); og
    2. indeholder bestemmelser om videreførsel af personoplysninger fra modtageren til tredjeparter, der befinder sig i et fremmed land;
  - (B) den registrerede giver sit samtykke til overførslen;

- (C) overførslen er nødvendig for opfyldelsen af en kontrakt mellem den registrerede og den ansvarlige part eller for gennemførelsen af foranstaltninger forud for kontraktindgåelsen, der er truffet som reaktion på den registreredes anmodning;
  - (D) overførslen er nødvendig for indgåelsen eller opfyldelsen af en kontrakt, der er indgået i den registreredes interesse mellem den ansvarlige part og en tredjepart, eller
  - (E) overførslen er til fordel for den registrerede, og:
    - 1. det ikke med rimelighed er praktisk muligt at indhente den registreredes samtykke til denne overførsel, og
    - 2. hvis det med rimelighed var praktisk muligt at indhente et sådant samtykke, ville den registrerede sandsynligvis give det.
2. I dette afsnit forstås ved:
- (A) "bindende virksomhedsregler" betyder politikker for behandling af personoplysninger inden for en virksomhedsgruppe, som overholdes af en ansvarlig part eller operatør inden for denne virksomhedsgruppe, når der overføres personoplysninger til en ansvarlig part eller operatør inden for den samme virksomhedsgruppe i et fremmed land; og
  - (B) "virksomhedsgruppe" betyder en kontrollerende virksomhed og dens kontrollerede virksomheder.