Standardkontraktsbestemmelser[[1]](#footnote-1)

i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger

mellem

Skoleindkøb

herefter ”den dataansvarlige”

og

KMD A/S

CVR nr. 26911745

Lautrupparken 40-42

2750 Ballerup

Danmark

herefter ”databehandleren”

der hver især er en ”part” og sammen udgør ”parterne”

HAR AFTALT følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

Indhold

[2. Præambel 3](#_Toc54674131)

[3. Den dataansvarliges rettigheder og forpligtelser 3](#_Toc54674132)

[4. Databehandleren handler efter instruks 4](#_Toc54674133)

[5. Fortrolighed 4](#_Toc54674134)

[6. Behandlingssikkerhed 5](#_Toc54674135)

[7. Anvendelse af underdatabehandlere 6](#_Toc54674136)

[8. Overførsel til tredjelande eller internationale organisationer 7](#_Toc54674137)

[9. Bistand til den dataansvarlige 7](#_Toc54674138)

[10. Underretning om brud på persondatasikkerheden 8](#_Toc54674139)

[11. Sletning og returnering af oplysninger 9](#_Toc54674140)

[12. Revision, herunder inspektion 9](#_Toc54674141)

[13. Parternes aftale om andre forhold 10](#_Toc54674142)

[14. Ikrafttræden og ophør 10](#_Toc54674143)

[15. Kontaktpersoner hos den dataansvarlige og databehandleren 11](#_Toc54674144)

[Bilag A Oplysninger om behandlingen 12](#_Toc54674145)

[Bilag B Underdatabehandlere 14](#_Toc54674146)

[B.3 Godkendte underdatabehandlere med særlige vilkår 15](#_Toc54674147)

[Bilag C Instruks vedrørende behandling af personoplysninger 16](#_Toc54674148)

[Bilag D Parternes regulering af andre forhold 27](#_Toc54674149)

# Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.
2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).
3. I forbindelse med leveringen af **’Aftale om levering af KMD Insight COVID-19 Portal’** inkl. alle tillæg, ændringer, tilkøb m.m. (”Aftalen”) behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.
4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.
10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

# Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[[2]](#footnote-2) nationale ret og disse Bestemmelser.
2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.
3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

# Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.
2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

Den dataansvarlige er herefter pligtig til at genoverveje lovligheden af instruksen. Parterne indgår dialog om instruksen og hvilke konsekvenser det kan få, hvis instruksen er ulovlig. Parterne drøfter om instruksen evt. kan tilrettes, så instruksen utvivlsomt bliver lovlig.

Den dataansvarlige indestår for, at dennes instrukser til databehandleren ikke strider med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.[[3]](#footnote-3)

# Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.
2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

# Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

* 1. Pseudonymisering og kryptering af personoplysninger
	2. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
	3. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
	4. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.
1. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.
2. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

# Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).
2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.
3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 3 måneders varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.
4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

1. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.
2. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.
3. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

# Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.
2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.
3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:
	1. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
	2. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
	3. behandle personoplysningerne i et tredjeland
4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.
5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

# Bistand til den dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

* 1. oplysningspligten ved indsamling af personoplysninger hos den registrerede
	2. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
	3. indsigtsretten
	4. retten til berigtigelse
	5. retten til sletning (”retten til at blive glemt”)
	6. retten til begrænsning af behandling
	7. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
	8. retten til dataportabilitet
	9. retten til indsigelse
	10. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
1. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:
2. den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet i Danmark, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder
3. den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder
4. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
5. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet i Danmark, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.
6. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

# Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 6 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.
3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:
	1. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
	2. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
	3. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.
4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

# Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.
2. Følgende regler i EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne efter ophør af tjenesterne vedrørende behandling af personoplysninger:

Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

# Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.
2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere~~t~~ angivet i Bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

# Parternes aftale om andre forhold

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

# Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.
3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.
4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.
5. Underskrift

På vegne af den dataansvarlige

Navn

Stilling

Telefonnummer

E-mail

Underskrift

På vegne af databehandleren

Navn René Hauge Sørensen

Stilling Business Line Director

Telefonnummer 22694771

E-mail res@kmd.dk

Underskrift

# Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

For den dataansvarlige:

Navn

Stilling

Telefonnummer

E-mail

For databehandleren:

Navn

Stilling

Telefonnummer

E-mail

# Bilag A Oplysninger om behandlingen

**A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige**

KMD foretager behandling af persondata for Kunden i forbindelse med Kundens screening af personale for Sars-CoV-2.

**A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)**

Databehandleren og databehandlerens underleverandør foretager på vegne af Kunden Sars-CoV-2 screening af personale samt drift, vedligehold og support af IT-løsningen til registrering af udførte test- og dokumentation af testresultater.

**A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede**

**Almindelige personoplysninger** (jf. databeskyttelsesforordningens artikel 6):

[x]  Almindelige personoplysninger

Data kan indeholde almindelige personoplysninger jf. databeskyttelsesforordningens artikel 6, stk. 1, herunder men ikke begrænset til identifikationsoplysninger, eksempelvis i form af CPR-nummer, pasoplysninger, CV, adresse og økonomiske oplysninger.

**Følsomme personoplysninger om** (jf. databeskyttelsesforordningens artikel 9):

[ ]  Race eller etnisk oprindelse

[ ]  Politisk overbevisning

[ ]  Religiøs overbevisning

[ ]  Filosofisk overbevisning

[ ]  Fagforeningsmæssigt tilhørsforhold

[ ]  Genetiske data

[ ]  Biometriske data

[x]  Helbredsoplysninger, herunder misbrug af medicin, narkotika, alkohol m.v.

[ ]  En fysisk persons seksuelle forhold eller seksuelle orientering

Idet screeningen indeholder testresultater for Sars-CoV-2 vil der være tale om behandling af helbredsoplytsninger.

**Personoplysninger om straffedomme og lovovertrædelser** (jf. databeskyttelsesforordningens artikel 10):

[ ]  Straffedomme

[ ]  Lovovertrædelser

**Oplysninger om cpr-nummer** (jf. databeskyttelseslovens § 11)

[x]  CPR-numre

**A.4. Behandlingen omfatter følgende kategorier af registrerede**

Data indeholder oplysninger om dataansvarliges medarbejdere, som har fået foretaget screening for Covid-19. Dvs. en registrering af, at der er foretaget screening, dato for screeningen og resultat af screeningen.

Kategorier af personoplysninger:

* Fuldt navn som på sundhedskort
* CPR-nummer
* Fødselsdato
* Køn
* Pasnr., kørekortnr. eller anden identifikation (Fx udlændinge)
* Telefonnummer
* Adresse for testlokation
* Kommentar (Tekstfelt)
* Tidspunkt for test
* Testtype
* Testsvar

**A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed**

Behandlingen er ikke tidsbegrænset og varer så længe, det er relevant for databehandlerens udførelse af de aftalte opgaver og efterlevelse af forpligtelser over for den dataansvarlige i Hovedaftalen.

**A.6. Den dataansvarliges overladelse af personoplysninger til databehandlerens behandling**

Den dataansvarlige har ansvaret for, at de personoplysninger, som den dataansvarlige instruerer databehandleren om at behandle, må behandles af databehandleren, herunder at behandlingen er nødvendig og legitim i forhold til den dataansvarliges opgavevaretagelse.

# Bilag B Underdatabehandlere

**B.1. Godkendte underdatabehandlere**

* Ved underskrift af Bestemmelserne godkender den dataansvarlige, at databehandleren videreoverlader behandling af de personoplysninger, som den dataansvarlige er dataansvarlig for, til én eller flere navngivne underdatabehandlere oplistet nedenfor, i overensstemmelse med databeskyttelsesforordningens artikel 28, stk. 2.
* De øvrige krav til databehandlernes behandling af de personoplysninger, som via databehandleren behandles på vegne af den dataansvarlige fremgår af nærværende aftale.
* Til brug for behandlingen vil databehandleren være berettiget til at anvende følgende underdatabehandlere (selvstændige juridiske enheder):

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere:

* Microsoft Ireland Operations Limited \* Atrium Building Block B, Carmenhall Road, Sandyford Industrial Estate \* Dublin 18, Ireland \* Attention: EOC Program Operations Dept.
* Microsoft Corporation \* One Microsoft Way, Redmond, WA 98056 \* USA
* Onlinecity.IO ApS (CVR-nr 27364276) \* Buchwaldsgade 50 \* 5000 Odense C \* Danmark

**B.2. Varsel for underretning om planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere, den dataansvarliges indsigelsesmulighed og behandling af sådan indsigelse**

B.2.1. Databehandleren skal pr. e-mail eller anden skriftlig vis til kontaktpersonen/kontaktpunktet anført i Bestemmelsernes punkt 0 underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer. Databehandleren kan stille krav om, at den dataansvarliges kontaktperson/kontaktpunkt tilmelder sig en digital meddelelsesordning hos databehandleren (og/eller databehandlerens underdatabehandlere) for at modtage underretning. En sådan underretning skal – så vidt muligt - være den dataansvarlige i hænde minimum 3 måneder før anvendelsen eller ændringen skal træde i kraft.

Hvis den dataansvarlige har indsigelser mod ændringerne, skal den dataansvarlige give meddelelse herom til databehandleren inden 30 dage efter modtagelsen af underretningen. Den dataansvarlige kan alene gøre indsigelse, hvis den dataansvarlige har rimelige, konkrete årsager hertil.

B. 2.2. Hvis den dataansvarlige afgiver en rimelig og konkret indsigelse mod anvendelse af en underdatabehandler inden for den anførte frist, er databehandleren forpligtet til at tage indsigelsen i betragtning. Hvis databehandleren vælger ikke at imødekomme indsigelse, eller hvis databehandleren ikke er i stand til at imødekomme indsigelse inden for en rimelig frist, er den dataansvarlige berettiget til med 1 måneds skriftligt varsel at opsige den del af Hovedaftalen dækkende netop den ydelse, hvor underdatabehandleren ellers ville få adgang til persondata. Den øvrige del af Hovedaftalen løber fortsat i henhold til bestemmelserne i Hovedaftalen.

B.2.3.Ved antagelse af nye underdatabehandlere i Bestemmelsernes løbetid, skal databehandleren iagttage de aftalte vilkår i punkt C.5 om lokalitet for behandling samt punkt C.6 om instruks vedrørende overførsel af personoplysninger til tredjelande.

## B.3 Godkendte underdatabehandlere med særlige vilkår

Databehandleren indestår for eventuelle underdatabehandleres ydelser på samme måde, som var de databehandlerens egne.

Såfremt databehandleren ved opfyldelsen af Hovedaftalen anvender ydelser fra underdatabehandlere, der er underlagt andre vilkår end de, der fremgår af eller svarer til vilkår i nærværende Bestemmelser, så er sådanne andre vilkår indeholdt i nærværende punkt B.3. Således finder alene de vilkår, som fremgår af nærværende punkt B.3, anvendelse for forholdet mellem databehandleren og den dataansvarlige vedrørende underdatabehandlerens behandling.

Til brug for behandlingen anvendes følgende underdatabehandlere med nedenstående særlige vilkår:

Microsoft Corporation \* One Microsoft Way, Redmond, WA 98056 \* USA

Vedlagt er aftale indgået af KMD på vegne af Kunden med Microsoft Corporation, One Microsoft Way, Redmond, WA 98056, USA, baseret på EU-kommissionens standardkontrakt.

Idet EU Kommissionens Standardkontraktsbestemmelser kræver, at den dataansvarlige er direkte part i Standardkontraktsbestemmelser, bemyndiges KMD til at indgå dette på vegne af Kunden.

Idet Microsoft Corporation er beliggende i et tredjeland, anvendes EU Kommissionens Standardkontraktsbestemmelser som gyldigt overførelsesgrundlag.

EU Kommissionens Standardkontraktsbestemmelser er således indgået af KMD på vegne af kunden med Microsoft Corporation og vedlagt.

Det fremgår af EU Kommissionens Standardkontraktsbestemmelser med Microsoft Corporation, at Microsoft Corporation er berettiget til at anvende og udskifte yderligere underdatabehandlere. Disse underdatabehandlere fremgår af Microsofts liste over underdatabehandlere og findes her: [LINK](https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downloadType=Document&downloadId=926b2cf5-6b6e-43ca-9bc3-f73e961aad5f&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913_Subprocessor_Listcommand=Download&downloadType=Document&downloadId=926b2cf5-6b6e-43ca-9bc3-f73e961aad5f?command=Download&downloadType=Document&downloadId=926b2cf5-6b6e-43ca-9bc3-f73e961aad5f&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913_Subprocessor_List)

Det fremgår endvidere, at Microsoft Corporation giver et varsel på 6 måneder før eventuelle nye underdatabehandlere ibrugtages. Dette sker ved, at Microsoft opdaterer ovennævnte liste og den Dataansvarlige skal gøre følgende for at modtage meddelelse herom:

På denne side: [Direkte link](https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3) (Data Protection Resources) sættes flueben foran “Microsoft Online Services Subprocessor List” derefter klikkes ”Save to Library”. Bemærk dette kræver sign-in.

Derefter vælges ”My Library” under ”More” tab’en øverst på skærmen.

Vælg ”Notification Settings” og indsæt her præference og e-mail.

# Bilag C Instruks vedrørende behandling af personoplysninger

**C.1. Behandlingens genstand/instruks**

**C.1.1. Behandlingens genstand/instruks**

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

Enhver behandling, som er nødvendig for, at databehandleren kan opfylde de i Hovedaftalen med bilag fastsatte forpligtelser, herunder alene:

Behandling af personoplysninger i forbindelse med Covid-19 screening.

Der henvises i øvrigt til Bilag A (Oplysninger om behandlingen).

**C.1.2. Ændringer i behandlingens genstand/instruks**

Hvis den dataansvarlige ønsker at ændre i behandlingens genstand/sin instruks til databehandleren - herunder hvis der f.eks. sker ændringer i de kategorier af personoplysninger, som databehandleren skal behandle på vegne af den dataansvarlige - skal dette ske i henhold til den mellem parterne aftalte proces for håndtering af ændringer af Hovedaftalen.

I det omfang sådanne ændringer er begrundet i den dataansvarliges forhold og medfører yderligere krav til databehandlerens gennemførelse af tekniske og organisatoriske foranstaltninger, iagttagelse af særlige individuelle vilkår eller i øvrigt merarbejde/meromkostninger/øgede risici for databehandleren, kan databehandleren kræve særskilt vederlag herfor, jf. bilag D.

Databehandleren er forpligtet til at levere sine ydelser i overensstemmelse med de aftalte ændringer, når ændringerne er implementeret.

**C.2. Behandlingssikkerhed**

**C.2.1. Sikkerhedsniveau**

C.2.1.1 Sikkerhedsniveauet skal afspejle:

Behandlingen omfatter en større mængde personoplysninger omfattet af databeskyttelsesforordningens artikel 9 om ”særlige kategorier af personoplysninger”, hvorfor der skal etableres et højt sikkerhedsniveau.

Databehandleren skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lov om behandling af personoplysninger.

Databehandleren skal på den dataansvarliges anmodning give den dataansvarlige tilstrækkelige oplysninger til, at denne kan påse, at de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger er truffet.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at sikre mod, at oplysninger hændeligt eller ulovligt tilintegøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab eller misbruges på baggrund af det etablerede (og aftalte) sikkerhedsniveau.

Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger (samt eventuelle udtrykkeligt specificerede foranstaltninger i Hovedaftalen), som er aftalt med den dataansvarlige, og som parterne er enige om er tilstrækkelige:

**C.2.1.1.1 PSEUDONYMISERING OG KRYPTERING AF PERSONOPLYSNINGER**

**Anvendelse af krypteringsteknologier**

I det omfang dette er et krav i henhold til gældende lov eller er specificeret udtrykkeligt i Hovedaftalen med den dataansvarlige, anvender databehandleren relevante krypteringsteknologier og andre lignende foranstaltninger under hensyntagen til risici og relevans.

**C.2.1.1.2 EVNEN TIL AT SIKRE VEDVARENDE FORTROLIGHED, INTEGRITET, TILGÆNGELIGHED OG ROBUSTHED AF BEHANDLINGSSYSTEMER OG –TJENESTER**

**Begrænsning af brugerprivilegier**

Databehandleren arbejder efter princippet om minimum brugerprivilegier (least privilege). Dette betyder at:

\*Alle brugerkonti hos databehandleren er underlagt princippet om minimumsrettigheder, der går på at begrænse en brugers adgang til et minimum hvormed de stadig kan udføre deres arbejde.

\*Kun personer, der er registreret og godkendt af databehandlerens Human Ressource afdeling, kan få tilladelse til at få adgang til databehandlerens information og systemer.

\*Databehandlerens brugere har kun bemyndigelse til at behandle oplysninger, der er relevante for deres arbejde.

**Opdeling af ansvar**

Alle databehandlerens brugerkonti er underlagt princippet om opdeling af ansvar (segregation of duties).

Adgangskontroller er opdelt i:

\*Adgangsanmodning

\*Adgangstilladelse

\*Adgangsadministration

Dette princip følges for så vidt muligt at begrænse risikoen for:

\*Misbrug eller utilsigtet ændring af data

\*At en og samme person både autoriserer og udfører handlinger

\*At en enkelt brugerkonto kan få adgang til, ændre eller bruge information uden tilladelse eller alarmering.

**Adgang til persondata og review**Brugeradgange hos databehandleren trækkes tilbage, hvis brugeren ikke længere opfylder adgangskriterierne. Adgangsrettigheder vurderes ved fastlagte intervaller, min hver 6. måned. Databehandleren håndterer autorisation til databehandlerens medarbejdere og, hvis det er aftalt i Hovedaftalen, for den dataansvarliges medarbejdere.

**Autentifikations mekanismer**
Databehandleren anvender passende logiske autentifikationsmekanismer, fx. adgangskoder, biometrics, multifaktor autentificering eller lignende mekanismer. De anvendte autentifikationsmekanismer efterlever, hvad der anses som god praksis indenfor feltet, såsom længde på adgangskode og kompleksitet.

**Uautoriseret adgang**
Databehandleren har passende tekniske foranstaltninger til at begrænse risikoen for uautoriseret adgang og/eller installation af ondsindet software. Sådanne foranstaltninger kan omfatte firewalls, anti-virus software og malware-beskyttelse. Databehandleren har formelle procedurer til sikring af, at sikkerhedssystemerne holdes opdaterede.

**Tilgængelighed**
Evne til at sikre tilgængelighed: Databehandleren tilstræber, at de behandlingssystemer og -tjenester, som anvendes til behandling af persondata for den dataansvarlige, og data deri, er tilgængelige på anmodning fra en autoriseret bruger.

**Change management**
Databehandleren har formelle change management procedurer for at sikre, at enhver ændring, på behørig vis, er autoriseret, testet og godkendt før den implementeres.

**Sletning af data ifm destruktion af medier og udstyr**

Databehandleren har formelle processer med henblik på at sikre, at der sker effektiv sletning af personoplysninger inden bortskaffelse af elektronisk udstyr.

**Beskyttelse af persondata i arbejdssituationer**
Databehandleren har implementeret en "clean desk" politik og beskyttelse af PC skærme i det offentlige rum for at beskytte mod uautoriseret adgang til persondata.

**Fortrolighedsaftaler**
Databehandleren kræver aftale om fortrolighed forud for al deling af intern og fortrolig information med eksterne parter inklusive kunder, leverandører, konsulenter og andre samarbejdspartnere.

Databehandlerens medarbejdere, der er involveret i behandling af persondata under denne Databehandleraftale, underlægges et ansvar om fortrolighed. Kun behørigt autoriserede medarbejdere gives adgang til persondata behandlet under denne Databehandleraftale.

Hvis der, i henhold til Hovedaftalen, kræves særlige sikkerhedsgodkendelser for medarbejdere, der er involveret i behandlingen af den dataansvarliges persondata, skal databehandleren sørge for, at sådanne godkendelser opnås.

**Betingelser for ansættelse og medarbejdertræning samt brug af underleverandører**
Den enkeltes ansvar for sikkerhed er klart defineret og beskrevet i alle databehandlerens medarbejderes ansættelseskontrakter. Databehandleren foretager en risikovurdering af og indgår en Sikkerhedsaftale med sine underleverandører forud for påbegyndelse af samarbejde.

Databehandleren sikrer, at dennes medarbejdere modtager tilstrækkelig træning og instrukser i relevante sikkerhedskontroller, fx. gennem obligatorisk e-learning.

**C.2.1.1.3 EVNEN TIL RETTIDIGT AT GENOPRETTE TILGÆNGELIGHEDEN AF OG ADGANGEN TIL PERSONOPLYSNINGER I TILFÆLDE AF EN FYSISK ELLER TEKNISK HÆNDELSE**

**Security Incident Management proces**

Databehandleren har implementeret en Security Incident Management proces med definerede procedurer for håndtering af sikkerhedssager, herunder brud på persondatasikkerhed.

Alle databehandlerens medarbejdere, eksterne konsulenter og samarbejdspartnere er ansvarlige for at rapportere sikkerhedssager. Styring af denne rapportering er defineret for at sikre klar kommunikation i organisationen og til databehandlerens leverandører og dataansvarlige.

**Business Continuity**

Databehandleren inkluderer informationssikkerhed (beskyttelse af confidentiality, integrity og availability, CIA) i sin proces for styring af Business Continuity. Der udføres Business Impact Analyse (BIA’er) som led i planlægning og vedligeholdelse af forretningskontinuitetsplaner.
Databehandleren har etableret en Plan for Business Continuity, der testes regelmæssigt.

Databehandleren sikrer, at muligheden for genetablering af data fra backup systemer testes regelmæssigt i et testmiljø. Genetablering skal yderligere testes efter større operationelle eller processuelle ændringer, der potentielt kan influere på backup rutiner.

**C.2.1.1.4 PROCEDURER FOR REGELMÆSSIG AFPRØVNING, VURDERING OG EVALUERING AF EFFEKTIVITETEN AF DE TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER TIL SIKRING AF BEHANDLINGSSIKKERHEDEN**

**Privatlivsindstillinger og Privacy Impact Assessment**

Databehandleren vedligeholder et overblik over alle sine behandlingsaktiviteter for den dataansvarlige. Det indgår heri, at privatlivsindstillinger for databehandlingen vurderes periodisk.

Yderligere gennemfører databehandleren en vurdering af personlige konsekvenser for den registrerede, en privacy impact assessment (PIA) og en samlet risikoscore fastsættes.

**C.2.1.1.5 ADGANG TIL OPLYSNINGERNE VIA INTERNETTET**

**Netværksbeskyttelse**

Databehandleren sikrer, at adgang til databehandlerens netværk og eksterne cloud baserede systemer er beskyttet af multifaktor autentificering, f.eks. i forbindelse med adgang til cloudmiljøer.

Databehandleren håndhæver automatisk timeout-session, baseret på en forud bestemt tidsperiode med inaktivitet, for eksterne forbindelser til databehandlerens systemer, primært servere og PC'er.

**C.2.1.1.6 BESKYTTELSE AF OPLYSNINGER UNDER TRANSMISSION**

**Brug af kryptografi under transmission**

Databehandleren bruger kryptografiske metoder til at overholde lovbestemmelser (fx. beskyttelse af personoplysninger under transmission).

**C.2.1.1.7 BESKYTTELSE AF OPLYSNINGER UNDER OPBEVARING**

**Sikkerhedskopiering**

Databehandleren sørger for sikkerhedskopiering og backup af systemer og data, og sikrer at sådanne sikkerhedskopier opbevares sikkert og i overensstemmelse med Hovedaftalens bestemmelser. Der gælder de samme retningslinjer for sikkerhedskopier som for al anden behandling af personoplysninger i medfør af Hovedaftalen og denne Databehandleraftale.

Sikkerhedskopier opbevares sikkert for at sikre, at sikkerhedskopier ikke går tabt i sager, der resulterer i tab af data fra det primære datacenter. Dette kan gøres ved at gemme sikkerhedskopier, der er geografisk adskilt fra det primære datacenter. Databehandleren kontrollerer regelmæssigt, at sikkerhedskopier er læsbare. Den dataansvarlige er ansvarlig for at verificere gendannet datas konsistens.

**C.2.1.1.8 FYSISK SIKRING AF LOKALITETER, HVOR DER BEHANDLES OPLYSNINGER**

**Fysiske adgangsbegrænsninger**

Databehandleren har etableret fysiske adgangsbegrænsninger. Områder, hvor personoplysninger behandles, er adskilt med adgangskontrolmekanismer fra områder med generel adgang. Sådanne mekanismer inkluderer eksempelvis systemer til fysisk adgangskontrol, låse, adgangskontrol-porte, sikkerhedsvagter og overvågningsudstyr.

**C.2.1.1.9 ANVENDELSE AF HJEMME-/FJERNARBEJDSPLADSER**

**Databehandlerens brug af hjemme-/ fjernarbejdspladser**

Databehandleren har etableret procedurer og kontroller til hjemme- og fjernarbejdspladser.
Databehandlerens medarbejdere har mulighed for udføre arbejde ved brug af fjernarbejdspladser (herunder hjemmearbejdspladser) med fjernadgang til databehandlerens it-systemer, forudsat at det udføres på en sikker måde:

1. Databehandlerens generelle sikkerhedsniveau skal altid opretholdes, når der arbejdes uden for databehandlerens fysiske lokationer
2. Kommunikationen, der bruges til fjernarbejde, skal være krypteret
3. Adgang må kun gives, hvis en anden faktor til godkendelse anvendes, såsom en fysisk token, SMS-adgangskode eller certifikat.

**C.2.1.1.10 LOGNING**

**Databehandlerens logning**

Aktiviteter, der udføres af databehandlerens systemadministratorer og operatører og andre med udvidede privilegier, logges som minimum med:

1. Dato
2. Bruger
3. Information om handling/aktivitet.

Databehandleren sikrer, at auditlogning bevares for en specifik periode. Et centralt Log Management system anvendes til formålet.

Databehandleren søger at beskytte logfaciliteter bedst muligt mod manipulation og tekniske fejl.

Databehandleren implementerer ur-synkronisering ved hjælp af NTP-servertjeneste til intern synkronisering.

Databehandleren overvåger logfiler i en sikkerhedsinformation og begivenhedsstyrings-løsning, der sigter mod at opdage generelle trusler mod databehandleren. Databehandleren kan implementere yderligere manuelle og automatiske logkontroller/overvågning for at overholde eventuelle aftalte kundespecifikke krav.

Databehandleren logger i øvrigt behandling af persondata i overensstemmelse med bestemmelserne i Hovedaftalen.

**C.2.1.1.11 SUPPLERENDE SIKKERHEDSFORANSTALTNINGER**

Der gælder ikke supplerende sikkerhedsforanstaltninger for løsningen.

**C.2.2. Den dataansvarliges orientering af databehandleren vedrørende behandlingsrisici**

Med henblik på, at databehandleren kan overholde sine forpligtelser i henhold til Bestemmelsernes punkt 6 skal den dataansvarlige orientere databehandleren

* hvis den dataansvarliges forhold (herunder f.eks. den dataansvarliges konkrete tilrettelæggelse af tekniske og organisatoriske foranstaltninger, den dataansvarliges konkrete anvendelse af databehandlerens leverance eller udfaldet af den dataansvarliges eventuelle konsekvensanalyse) fordrer, at der foretages ændringer i databehandlerens tekniske eller organisatoriske foranstaltninger med henblik på opfyldelse af databeskyttelsesforordningens kapitel II, eller at der udarbejdes og implementeres supplerende foranstaltninger, der understøtter indbygget databeskyttelse og databeskyttelse gennem indstillinger,
* hvis der i Bestemmelsernes løbetid sker en ændring af den risiko, som behandlingsaktiviteterne udgør, eller
* hvis den dataansvarlige i øvrigt måtte ønske gennemførelse af yderligere foranstaltninger.

**C.2.3. Nye eller ændrede krav til databehandlerens tekniske og organisatoriske foranstaltninger**

Hvis principperne i Bestemmelsernes punkt 6 - herunder bl.a. sammenholdt med den dataansvarliges ovenstående orientering - medfører nye eller ændrede krav til tekniske og organisatoriske foranstaltninger, set i forhold til, hvad der er anført ovenfor i nærværende punkt C.2.1 eller i Hovedaftalen, skal den dataansvarlige godtgøre databehandleren omkostningerne hertil, jf. bilag D. I det omfang databehandleren påtager sig at gennemføre ændringer i tekniske og organisatoriske foranstaltninger ensartet for alle sine kunder, herunder i f.t. den dataansvarlige i nærværende Bestemmelser, og databehandleren er enig i, at ændringerne udgør passende foranstaltninger, skal databehandleren gennemføre sådanne ændringer uden beregning for den dataansvarlige.

Hvor parterne skal aftale og udføre implementering af ændringer afledt af nærværende punkt C. 2, skal dette følge den af parterne aftalte proces for håndtering af ændringer af Hovedaftalen. Databehandleren er forpligtet til at levere sine ydelser i overensstemmelse med de aftalte ændringer, når ændringerne er implementeret.

**C.3 Bistand til den dataansvarlige**

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

**Begæring vedrørende registreredes rettigheder**

Databehandleren skal uden unødig forsinkelse, efter at være blevet opmærksom herpå, skriftligt underrette den dataansvarlige om enhver anmodning rettet til databehandleren eller dennes underdatabehandlere fra en registreret om udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret. Databehandleren er ikke berettiget til at besvare anmodninger fra en registreret vedrørende udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret. Databehandleren skal på anmodning fra den dataansvarlige hjælpe med at opfylde den dataansvarliges forpligtelser i forhold til de registreredes rettigheder i henhold til gældende databeskyttelsesret.

**Databehandlerens information om brud på persondatasikkerhed til den dataansvarlige, jf. punkt 10.4 i Databehandleraftalen**

Det påhviler databehandleren at underrette den dataansvarlige hurtigst muligt og uden unødig forsinkelse efter at være blevet bekendt med et brud på persondatasikkerheden. Underretningen vil om muligt indeholde følgende oplysninger:

1. En beskrivelse af hændelsen, herunder hvor den fysisk fandt sted.
2. Et hændelsesforløb, indeholdende information om hændelsens start, konstatering og (forventet) afslutning.
3. Karakteren af bruddet på persondatasikkeheden, herunder eventuelt involveret teknologi, kategorierne af oplysninger og registrerede samt det omtrentlige antal berørte registrerede og om muligt det omtrentlige antal registreringer.
4. En generel vurdering af den sandsynlige konsekvens for de registrerede.
5. En beskrivelse af de foranstaltninger, som databehandleren har truffet eller/og foreslår truffet af den dataansvarlige for at håndtere hændelsen og begrænse bruddets skadevirkninger.
6. Oplysning om, at underretningen er endelig, eller om og hvordan der vil følge yderligere information.
7. Oplysning om, hvor den dataansvarlige kan få yderligere information.

**Bistand i øvrigt efter punkt 9.1 og 9.2 i Databehandleraftalen**

På den dataansvarliges anmodning bistår databehandleren - under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren – i rimeligt omfang med input/bidrag til den dataansvarliges udførelse af sine opgaver og overholdelse af sine forpligtelser anført i punkt 9.1 og 9.2 i Bestemmelserne.

Såfremt den dataansvarlige vurderer, at behandlingen sandsynligvis vil indebære en høj risiko for de registreredes rettigheder og frihedsrettigheder, skal databehandleren på anmodning fra den dataansvarlige bistå den dataansvarlige ifm. dennes forpligtelser efter databeskyttelsesforordningens artikel 35 og 36 ved at indgive de oplysninger til den dataansvarlige, der er nødvendige for, at den dataansvarlige kan foretage en konsekvensanalyse i overensstemmelse med artikel 35 og foretage en forudgående høring af Datatilsynet i overensstemmelse med artikel 36.

Databehandleren skal endelig sikre, at dennes tekniske og organisatoriske foranstaltninger gør det muligt for den dataansvarlige at overholde sine forpligtelser efter databeskyttelsesforordningens art. 33-36, herunder f.eks. ved passende foranstaltninger vedr. styring af sikkerhedsbrud, styring af aktiver, logning mv.

**Vederlag for bistand**

Den dataansvarlige betaler særskilt vederlag for bistand efter nærværende punkt C.3 og aftaler parterne ikke andet, så skal sådan bistand afregnes efter medgået tid og materialer, jf. bilag D. I tilfælde af brud på persondatasikkerhed, som databehandleren har ansvaret for, bistår databehandleren i relation til punkt 9.2.a og 9.2.b i Bestemmelserne dog uden beregning med information om bruddet på persondatasikkerhed, jf. punkt 10.4 i Bestemmelserne og ovenfor i nærværende punkt C.3, og med at udfinde de berørte registrerede, hvis den dataansvarlige ikke selv er i stand til dette.

Databehandlerens timeforbrug forbundet med vederlagsberretigende bistand efter skal dog altid være rimeligt set i forhold til det udførte arbejde. Forud for påbegyndelse af opgaver skal databehandlerens estimerede vederlag herfor godkendes af den dataansvarlige. Dette gælder dog ikke, hvis opgavens karakter forudsætter, at databehandleren handler straks. I sådanne situationer, skal databehandleren hurtigst muligt derefter indhente den dataansvarliges skriftlige godkendelse af det estimerede vederlag for opgaven. Såfremt arbejdet med udførelsen af opgaverne overstiger det godkendte estimat, skal databehandleren straks orientere den dataansvarlige herom, herunder skal databehandleren redegøre for baggrunden for, at det estimerede vederlag overstiges.

**C.4 Opbevaringsperiode/sletterutine**

Hvor ikke andet er aftalt, så opbevares personoplysninger, som databehandleren behandler på den dataansvarliges vegne, hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne tilbageleveret og/eller slettet.

Senest ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren tilbagelevere alle personoplysninger, som databehandleren behandler på den dataansvarliges vegne, og slette eksisterende kopier i overensstemmelse med Hovedaftalen samt punkt 11 i Bestemmelserne. På anmodning fra den dataansvarlige skal databehandleren skriftligt bekræfte, at sletning er foretaget.

**C.5 Lokalitet for behandling**

Nærmere oplysninger om behandlingssteder for databehandleren og dennes underdatabehandlere kan fås ved henvendelse hos databehandleren. Oplysningerne kan udleveres i det omfang udlevering kan ske uden sikkerhedsmæssig risiko efter databehandlerens vurdering. I sådanne tilfælde udleveres da i udgangspunktet kun oplysninger om land og by for databehandlingsstedet.

Databehandleren er berettiget til at overføre eller tillade overførsel af personoplysninger til behandling uden for Danmark. Mht. behandling i tredjelande se punkt C.6 nedenfor.

**C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande**

Databehandleren er berettiget til at anvende underdatabehandlere beliggende i tredjelande til opfyldelse af databehandlerens forpligtelser overfor den dataansvarlige.

Anvendelse af underdatabehandlere beliggende i tredjelande kan alene ske, hvis (i) overførslen er baseret på en afgørelse fra EU Kommissionen om tilstrækkelighed af beskyttelsesniveau, herunder f.eks. at det pågældende tredjeland mv. har et tilstrækkeligt beskyttelsesniveau, (ii) overførslen er omfattet af fornødne garantier, som f.eks. EU Kommissionens Standardkontraktsbestemmelser eller iii) overførslen er omfattet af relevante bindende virksomhedsregler. Såfremt det i henhold til det anvendte overførselsgrundlag kræves, at den dataansvarlige er direkte part i overførselsgrundlaget, skal databehandleren anses for bemyndiget til at etablere og indgå dette på vegne af den dataansvarlige. Databehandleren er berettiget til at overdrage denne bemyndigelse til underdatabehandlere, således at underdatabehandlerne kan etablere og indgå et retligt overførselsgrundlag på vegne af den dataansvarlige.

Af punkt B.1. i bilag B fremgår de underdatabehandlere i tredjelande med tilhørende overførselsgrundlag, som den dataansvarlige har godkendt brugen af, og som databehandleren dermed er berettiget til – og instrueret om - at overføre personoplysninger til, ved Bestemmelsernes ikrafttræden.

Såfremt der som overførselsgrundlag anvendes EU Kommissionens Standardkontraktsbestemmelser, vedlægges kopi af de af databehandleren på vegne af den dataansvarlige indgåede EU Kommissionens Standardkontraktsbestemmelser (EU standardkontrakt) i et ”Bilag C - underbilag 1” til dette bilag C. EU standardkontrakten vil alene finde anvendelse for den del af ydelserne og behandlingen under Hovedaftalen, der udføres i henhold til EU standardkontraktsbestemmelserne. Øvrigt indhold i nærværende Bestemmelser skal ikke anses for at ændre på indholdet af den vedlagte EU standardkontrakt i Bilag C - underbilag 1.

Databehandleren er af den dataansvarlige bemyndiget til at indgå aftale om ændringer til den i Bilag C - underbilag 1 indeholdte EU standardkontrakt som følge af ændringer i databeskyttelseslovgivningen som disse implementeres af databehandleren eller underdatabehandleren i tredjelandet. Eventuelle ændringer vil alene blive udført i overensstemmelse med de til enhver tid gældende EU-regler for brug af EU Kommissionens Standardkontraktsbestemmelser. Den til enhver tid gældende version af den indgåede EU standardkontrakt kan udleveres efter anmodning til databehandleren.

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsels af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

Parterne er enige om at følge den i punkt B.2 i bilag B anførte proces vedrørende tilføjelse eller udskiftning af underdatabehandlere i tredjelande. Den dataansvarliges instruks omfatter således også overførsel af personoplysninger til nye underdatabehandlere i tredjelande, der i Bestemmelsernes løbetid antages af databehandleren i overensstemmelse med den i punkt B.2 i bilag B anførte proces og nærværende punkt C.6.

**C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren**

Databehandleren er certificeret efter ISO27001-standarden og har implementeret en kontrolramme i overensstemmelse med ISO27002 og databeskyttelsesforordningen. Databehandleren sender på den dataansvarliges anmodning kopi af sit SoA dokument (Statement of Applicability) til den dataansvarlige til orientering. Alternativt kan databehandleren vælge at stille SoA-dokumentet elektronisk til rådighed.

Databehandleren får for egen regning hvert år udarbejdet en erklæring fra en uafhængig statsautoriseret revisor om databehandlerens overholdelse af generelle it-kontroller. Erklæringen vedrører generelle it-kontroller i f.t. databehandlerens standard processer og ydelser i Danmark. Erklæringen er en ISAE 3402 type 2-erklæring, eller erklæringer der måtte træde i stedet for denne.

Databehandleren får endvidere for egen regning hvert år udarbejdet en generel erklæring fra en uafhængig statsautoriseret revisor vedrørende databehandlerens behandlingssikkerhed i relation til persondata. Erklæringen vedrører udførte kontroller i f.t. databehandlerens standardprocesser og -ydelser i Danmark og med udgangspunkt i databehandlerens standard databehandleraftale. Erklæringen bliver udarbejdet som en ISAE 3000-erklæring type 2-erklæring, eller erklæringer der måtte træde i stedet for denne.

Databehandleren sender vederlagsfrit på den dataansvarliges anmodning uden unødig forsinkelse disse revisionserklæringer til den dataansvarlige til orientering. Alternativt kan databehandleren vælge at stille revisionserklæringerne elektronisk til rådighed.

Baseret på resultaterne af databehandlerens revisionserklæringer, jf. ovenfor, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Sådanne anmodninger håndteres i overensstemmelse med punkt C.2 i nærværende bilag ovenfor.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, efter forudgående aftale med databehandleren og normalt med et skriftligt varsel på mindst 10 arbejdsdage, når den dataansvarlige finder det nødvendigt, dog makismalt én gang årligt. Hvor den dataansvarlige besigtiger databehandlerens lokationer, skal den dataansvarlige acceptere databehandlerens rimelige krav til sikkerhed og fortrolighed. Hvor den dataansvarlige anvender tredjepart til inspektion, indestår den dataansvarlige for, at tredjeparten accepterer og overholder databehandlerens rimelige krav til sikkerhed og fortrolighed. Den dataansvarlige kan ikke anvende tredjeparter til inspektion uden databehandlerens godkendelse. Databehandleren må alene nægte godkendelse af saglige årsager, herunder men ikke begrænset til, at tredjeparten er en konkurrent.

Den dataansvarlige skal godtgøre databehandlerens tid og omkostninger i forbindelse med tilsyn (f.eks. fysiske inspektioner, skriftlig informationsindsamling og besvarelse af spørgeskemaer), og aftaler parterne ikke andet, så afregnes databehandlerens medvirken til tilsyn efter medgået tid og materialer, jf. bilag D.

**C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere**

Tilsyn kan f.eks. ske ved skriftlig informationsindsamling eller i form af en fysisk inspektion af lokaliteterne, hvorfra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen, med henblik på at fastslå underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Ud over det planlagte tilsyn, kan databehandleren gennemføre en inspektion, fx i form af skriftlig informationsindsamling eller fysisk besøg, med underdatabehandleren, når databehandleren (eller den dataansvarlige) finder det nødvendigt.

Såfremt underdatabehandleren får udarbejdet en årlig revisionserklæring fra en uafhængig tredjepart angående underdatabehandlerens overholdelse af underdatabehandleratalen og de heri aftalte tekniske og organisatoriske sikkerhedsforanstaltninger, skal databehandleren modtage kopi heraf. Databehandleren gennemgår revisionserklæringen og følger op på eventuelle forhold, der giver anledning til yderligere undersøgelser.

Databehandleren dokumenterer afholdte tilsyn. Dokumentation for afholdte tilsyn udmøntes normalt i en tilsynsrapport indeholdende beskrivelse af scope, væsentlige findings og plan for eventuelle mitigerende foranstaltninger. På den dataansvarliges anmodningfremsendes kort opsummering af tilsynet uden unødig forsinkelse til den dataansvarlige til orientering. Alternativt kan databehandleren vælge at stille kort opsummering af tilsynet elektronisk til rådighed.

Baseret på resultaterne af tilsynet, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Sådanne anmodninger følger hovedkontrakens paragraf 5.6. Audit

Den dataansvarlige kan – hvis det findes nødvendigt – vælge at initiere og deltage på en fysisk inspektion hos underdatabehandleren. Dette kan blive aktuelt, hvis den dataansvarlige vurderer, at databehandlerens inspektion hos underdatabehandleren ikke har givet den dataansvarlige tilstrækkelig sikkerhed for, at behandlingen hos underdatabehandleren sker I overensstemmelse med databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Sådan inspektion gennemføres efter forudgående aftale med databehandleren/underdatabehandleren og normalt med et skriftligt varsel på mindst 10 arbejdsdage til databehandleren/underdatabehandleren.

Hvor den dataansvarlige besigtiger underdatabehandlerens lokationer, skal den dataansvarlige acceptere underdatabehandlerens rimelige krav til sikkerhed og fortrolighed. Hvor den dataansvarlige anvender tredjepart til inspektion, indestår den dataansvarlige for, at tredjeparten accepterer og overholder underdatabehandlerens rimelige krav til sikkerhed og fortrolighed. Den dataansvarlige kan ikke anvende tredjeparter til inspektion uden underdatabehandlerens godkendelse. Underdatabehandleren må alene nægte godkendelse af saglige årsager, herunder men ikke begrænset til, at tredjeparten er en konkurrent.

Den dataansvarliges eventuelle deltagelse i et tilsyn hos underdatabehandleren ændrer ikke ved, at databehandleren også herefter har det fulde ansvar for underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

# Bilag D Parternes regulering af andre forhold

**D.0 Modifikationer til Bestemmelserne**

D.0.1

Bestemmelserne benævnes også ”Databehandleraftalen”.

D.0.2

Databehandleraftalen indgås som tillæg eller bilag til Hovedaftalen.

D.0.3

Punkt 2.4 skal forstås således, at Databehandleraftalen har forrang i forhold til eventuelle tilsvarende bestemmelser i Hovedaftalen mellem Parterne – men ikke evt. andre aftaler mellem Parterne, der vedrører databehandling til andre formål.[[4]](#footnote-4)

D.0.4

I punkt 6.3 sidste punktum ændres ”bilag C” til ”bilag D”. [[5]](#footnote-5)

D.0.5

I relation til punkt 7.3, 2. punktum:

* ændres ”mindst 3 måneders varsel” til ”så vidt muligt mindst 3 måneders varsel” [[6]](#footnote-6) og
* tilføjes til slut ”jf. punkt B.2 i Bilag B”. [[7]](#footnote-7)

I relation til punkt 7.3, 3. punktum:

* ændres ”Længere varsel” til ”Andet varsel” [[8]](#footnote-8).

D.0.6

Teksten i punkt 7.6 udgår.[[9]](#footnote-9)

D.0.7

Teksten i punkt 14.1 erstattes med: ”Bestemmelserne træder i kraft på datoen for begge parters underskrift af Hovedaftalen, hvortil Bestemmelserne er knyttet som bilag.”

Parterne er således enige om, at Bestemmelserne (dvs. Databehandleraftalen) ikke underskrives særskilt af parterne i punkt 14.5. [[10]](#footnote-10)

D.0.8

Til punkt 14.2 føjes til slut: ”Eventuelle ændringer håndteres som udgangspunkt i h.t. regler for ændringshåndtering i Hovedaftalen” [[11]](#footnote-11)

D.0.9

Teksten i punkt. 15.1 erstattes med: ”Parterne kan kontakte hinanden via de kontaktpersoner, som fremgår af bilag D.[[12]](#footnote-12)

D.0.10

Modifikationerne i nærværende punkt D.0 med underpunkter har forrang for øvrige dele af Bestemmelserne.

D.0.11

Til punkt C.4 tilføjes: ”På baggrund af journalføringsbekendtgørelsen (BEK nr. 530 af 24/05/2018 Bekendtgørelse om autoriserede sundhedspersoners patientjournaler), foreskrives opbevaring af helbredsoplysninger, herunder testsvar, i 10 år.”

D.0.12

I henhold til lovbekendtgørelse 1444 af 1. oktober 2020 (Bekendtgørelse af lov om foranstaltninger mod smitsomme og andre overførbare sygdomme) §21a, §22b og §26, samt bekendtgørelse 1919 af d. 11. december 2020 (Bekendtgørelse om private testudbyderes anmeldelse af positive resultater af test for COVID-19 med henblik på smitteopsporing og kompensation), kræves det at alle testresultater indrapporteres til SSI, Sundhed.dk, egen læge, COVID-19 pas/MinSundhed-APP samt at positive test indrapporteres til smitteopsporing ved Styrelsen for Patientsikkerhed.

Følgende data vil blive indrapporteret:

* Personlig identifikation på de testede (herunder CPR-nummer og kontaktinfo).
* Oplysninger om udførte tests (testmetode, testtidspunkt, testlokation samt testresultat)

På baggrund af journalføringsbekendtgørelsen (BEK 1090 af 28. juli. 2020 Bekendtgørelse om autoriserede sundhedspersoners patientjournaler §15), gøres der desuden opmærksom på at muligheden for sletning af data bortfalder, idet bekendtgørelsen foreskriver opbevaring af helbredsoplysninger, herunder testsvar, i 10 år.

Vi gør opmærksom på, at det er Kundens ansvar at sikre, at de personer der testes, er informeret om, og giver samtykke til, at data videregives til SSI (for alle test) og til smitteopsporing (for positive test) hos Styrelsen for Patientsikkerhed. KMD er lovgivningsmæssig forpligtet til at indrapportere disse informationer, hvorfor accept af dette er en forudsætning for test.

SSI videregiver data til sundhed.dk og egen læge, hvis den enkelte person der testes giver samtykke til dette.

Eventuelt samtykke gives på tidspunktet for podningen.

**D.1. Den dataansvarliges øverste sikkerhedsansvarlige og eventuelle databeskyttelsesrådgiver (DPO)**

Det påhviler den dataansvarlige at indberette den dataansvarliges øverste sikkerhedsansvarlige, samt substitut herfor, i relation til opgaver, som databehandleren løser for den dataansvarlige. Hvis den dataansvarlige har en databeskyttelsesrådgiver (DPO), så påhviler det endvidere den dataansvarlige at give oplysning om databeskyttelsesrådigiveren (DPO’en). Endeligt påhviler det den dataansvarlige at give oplysning om, hvem der skal underrettes ved brud på persondatasikkerheden. Den dataansvarlige skal således give meddelelse om navn, titel, kontoradresse, e-mail samt direkte telefonnummer på øverste sikkerhedsansvarlig, substitut, kontaktperson ved brud på persondatasikkerheden og eventuelle databeskyttelsesrådgiver (DPO) til databehandlerens Security Incident Respons Team på SIRT@KMD.dk. Den dataansvarlige skal give databehandleren besked om ændringer på tilsvarende vis.

**D.2. Gældende lovgivning**

Databehandlerens behandling af personoplysninger er underlagt persondatalovgivningen i Danmark.

Hvis den dataansvarliges brug af databehandlerens tjeneste og beskaffenheden af den dataansvarliges personoplysninger om de registrerede medfører, at persondataretlig regulering for andre lande end Danmark vil være gældende for behandlingen, påhviler det den dataansvarlige at oplyse databehandleren herom samt aftale særlige individuelle vilkår med databehandleren om, hvilke yderligere foranstaltninger, dette måtte medføre for databehandleren. Eventuelle omkostninger, som databehandleren måtte blive påført som følge heraf, skal afholdes af den dataansvarlige. Databehandleren er dog ansvarlig for at afdække og sikre overholdelsen af yderligere databeskyttelsesretlig regulering, der påhviler denne eller dennes underdatabehandlere som følge af databehandlerens valg af underdatabehandlere.

**D.3. Betaling af særskilt vederlag/afholdelse af KMD’s omkostninger**

Hvor den dataansvarlige skal betale særskilt vederlag/afholde KMD’s omkostninger i henhold til Bestemmelserne, skal dette ske efter medgået tid og materialer, medmindre andet udtrykkeligt er aftalt. Hvor parterne i Hovedaftalen har aftalt timepriser for databehandlerens konsulenter samt betalingsvilkår for levering af konsulentydelser efter medgået tid og materialer, skal sådanne timepriser og betalingsvilkår anvendes. Hvor parterne ikke i Hovedaftalen har aftalt timepriser eller betalingsvilkår for levering af konsulentydelser efter medgået tid og materialer, skal databehandleren afregne den dataansvarlige i henhold til databehandlerens til enhver tid generelt gældende timepriser og fakturere den dataansvarlige herfor månedsvis bagud.

Databehandlerens timeforbrug forbundet med vederlagsberretigende bistand efter skal dog altid være rimeligt set i forhold til det udførte arbejde. Forud for påbegyndelse af opgaver skal databehandlerens estimerede vederlag herfor godkendes af den dataansvarlige. Dette gælder dog ikke, hvis opgavens karakter forudsætter, at databehandleren handler straks. I sådanne situationer, skal databehandleren hurtigst muligt derefter indhente den dataansvarliges skriftlige godkendelse af det estimerede vederlag for opgaven. Såfremt arbejdet med udførelsen af opgaverne overstiger det godkendte estimat, skal databehandleren straks orientere den dataansvarlige herom, herunder skal databehandleren redegøre for baggrunden for, at det estimerede vederlag overstiges.

1. Læsevejledning:

KMD’s udfyldelse af Bestemmelserne fremgår med grå skrift.

I bilag D punkt D.0 fremgår enkelte modifikationer til Bestemmelserne, der er nødvendige i f.t. klarhed samt KMD’s leverance set up og måde at foretage databehandling på. I fodnoter er begrundelsen for KMD’s modifikationer til Bestemmelserne angivet.

KMD har valgt også at kalde Bestemmelserne for ”Databehandleraftalen”.

Hvis den dataansvarlige måtte have særlige individuelle krav eller ønske om individuelle modifikationer til Databehandleraftalen (inkl. bilag), så bedes sådanne anført til slut i bilag D under et punkt med overskriften ”For denne Databehandleraftale gælder følgende særlige individuelle vilkår”. Bemærk, KMD’s accept af den dataansvarliges individuelle krav forudsætter, at der forud for indgåelse af Databehandleraftalen opnås leverancetilsagn internt i KMD til individuel administration. Individuelle krav vil blive prissat særskilt. [↑](#footnote-ref-1)
2. Henvisninger til ”medlemsstat” i disse bestemmelse skal forstås som en henvisning til ”EØS medlemsstater”. [↑](#footnote-ref-2)
3. Teksten angiver, hvordan parterne skal forholde sig i tilfælde af, at databehandleren underretter den dataansvarlige om, at en instruks efter databehandlerens mening er i strid med databeskyttelsesreglerne. Teksten er indsat som supplement til punkt 4.2, i overensstemmelse med Datatilsynets note til bestemmelsen. [↑](#footnote-ref-3)
4. Herved præciseres, at Databehandleraftalen vedrører og har forrang for Hovedaftalen, som defineret i punkt. 2.3. i Databehandleraftalen – og ikke andre aftaler mellem parterne. Hvis Parterne har indgået/indgår aftaler om andre leverancer, så skal Parterne indgå separate databehandleraftaler vedrørende databehandlinger i sådanne leverancer. [↑](#footnote-ref-4)
5. Den dataansvarlige har i bilag C punkt C.2 beskrevet de sikkerhedsforanstaltninger, som den dataansvarlige standardmæssigt tilbyder ved levering af løsningen/leverancen til den dataansvarliges kunder. Hvis den dataansvarlige måtte have supplerende særlige individuelle krav, herunder f.eks. krav til yderligere foranstaltninger, så bedes sådanne (af hensyn til KMD’s individuelle administration) anført til slut i bilag D under et punkt med overskriften ”For denne Databehandleraftale gælder følgende særlige individuelle vilkår”. Bemærk, KMD’s accept af den dataansvarliges individuelle krav forudsætter, at der forud for indgåelse af Databehandleraftalen opnås leverancetilsagn internt i KMD til individuel administration. Individuelle krav vil blive prissat særskilt. [↑](#footnote-ref-5)
6. Databehandleren vil *så vidt muligt* søge skriftligt at underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 3 måneders varsel. Databehandleren kan dog ikke love, at alle databehandlerens underdatabehandlere har påtaget sig en varslingspligt på netop ”mindst 3 måneder” over for databehandleren. Endvidere kan det ikke udelukkes, at databehandleren undtagelsesvis kan få behov for hurtig udskiftning af en underdatabehandler fx i tilfælde af, at en underdatabehandler ikke performer tilfredsstillende efter databehandlerens opfattelse. [↑](#footnote-ref-6)
7. Bestemmelsen suppleres af uddybende regulering i bilag B. [↑](#footnote-ref-7)
8. Andet varsel – dvs. såvel længere som kortere varsel - kan fremgå af bilag B. [↑](#footnote-ref-8)
9. Bestemmelsen er slettet, fordi KMD’s underdatabehandlere generelt ikke tilbyder at påtage sig sådant vilkår overfor KMD. Vilkåret indgår derfor normalt ikke i underdatabehandleraftaler mellem KMD og KMD’s underdatabehandlere. Efter KMD’s opfattelse, så er rækkevidden af punkt. 7.6 og den praktiske sikring af begunstigelsen usikker – og medtagelse af bestemmelsen ville næppe give den dataansvarlige en bedre ret end den dataansvarlige allerede har efter gældende konkurs- og databeskyttelsesret. [↑](#footnote-ref-9)
10. Parterne indgår og underskriver Hovedaftale, hvortil nærværende Databehandleraftale indgår som et bilag. Det er derfor ikke nødvendigt, at Databehandleraftalen underskrives selvstændigt. [↑](#footnote-ref-10)
11. I mangel af anden regulering vedrørende ændringshåndtering i Databehandleraftalen, så angives her, at ændringer til Databehandleraftalen som udgangspunkt sker i h.t. regler for ændringshåndtering i Hovedaftalen. [↑](#footnote-ref-11)
12. Parternes kontaktpersoner fremgår i bilag D. Det er lettere for parterne at ajour holde parternes kontaktpersoner, hvis de fremgår i bilag D. [↑](#footnote-ref-12)