Changelog

VERSION	ÆNDRINGER
1.1	Ændringer i Bestemmelserne 7.7., 9.2., 10.4. og Bilag C.8. *(Tastefejl og opdaterede krydshenvisninger).*

UDKAST

Standardkontraktsbestemmelser

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

mellem

[NAVN]
CVR [CVR-NR]
[ADRESSE]
[POSTNUMMER OG BY]
[LAND]

herefter "den dataansvarlige"

og

MedCom
CVR 26919991
Forskerparken 10
5230 Odense M
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

1. Indhold

2. 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 Tilslutning til VDX (Videoknudepunktet) jf. den indgåede tilslutningsaftale 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.

3. 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[1] nationale ret og disse Bestemmelser.

1 Henvisninger til "medlemsstat" i disse bestemmelse skal forstås som en henvisning til "EØS medlemsstater".

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.

4. 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.

5. 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.

6. 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:

   a. Pseudonymisering og kryptering af personoplysninger

b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

2. 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.

3. 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.

7. 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.

5. 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.

6. 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.

7. 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.

8. 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:

    a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
    b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
    c. 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.

9. 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:

   a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
   b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
   c. indsigtsretten
   d. retten til berigtigelse
   e. retten til sletning ("retten til at blive glemt")
   f. retten til begrænsning af behandling
   g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
   h. retten til dataportabilitet
   i. retten til indsigelse
   j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

2. 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:

   a. 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, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

   b. 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

c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, 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.

3. 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.

10. 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 24 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:

   a. 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

   b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

   c. 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.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

12. 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 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.

13. 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.

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.

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 skriftligt varsel af begge parter.

5. Underskrift

   På vegne af den dataansvarlige

Navn	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-mail	[E-MAIL]
Underskrift	

   På vegne af databehandleren

Navn	Lars Hulbæk
Stilling	Direktør
Telefonnummer	4036 8615
E-mail	lhf@medcom.dk
Underskrift	

15. 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.

Navn	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-mail	[E-MAIL]

Navn	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-mail	vdx@medcom.dk

Bilag A Oplysninger om behandlingen

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

Formålet med Databehandlingen i VDX (videoknudepunktet) er inden for det definerede formål for VDX at understøtte de Dataansvarliges behov for at afholde videomøder.

Databehandleren er kontraktholder og fællesoffentlig systemforvalter for VDX.

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

Databehandlingen består i VDX består i transmission af videostrømme med personoplysninger. Transmissionen sker på baggrund af den Dataansvarliges instruks.

Instruks for transmissionen af personoplysninger i VDX sker, når den Dataansvarlige booker et videomøde i VDX. Transmissionen sker i overensstemmelse med den konfiguration, som bookingen resulterer i.

Der gemmes ikke og tages ikke backup af selve videostrømmene.

Herudover består databehandlingen i opbevaring af personoplysninger i en række støttesystemer, herunder et VDX API for administration, booking og integration til lokale fag- og bookingsystemer og specialudviklede applikationer samt integration til lokal brugerstyring.

Databehandleren hoster, drifter, vedligeholder, overvåger og supporterer VDX gennem Underdatabehandlere.

Databehandleren behandler personoplysninger om brugere af VDX API'et for, at brugerne kan være oprettet og have adgang til VDX API'et, hvori de Dataansvarlige selv administrerer og forvalter egen organisation og booking af videomøder.

Databehandleren behandler personoplysninger om VDX API'ets brugere for at understøtte sikkerheden med logning.

Databehandleren behandler personoplysningerne om brugerne i VDX-API'et for udsendelse af servicemeddelelser om drift og vedligehold af VDX.

Databehandleren modtager alarmer om anomalier i overvågningen af VDX.

Databehandleren foretager sletning i samarbejde med Underdatabehandler ved nedlæggelse af en tilslutning til VDX.

Databehandler bistår Underdatabehandleren med at løse supporthenvendelser for VDX.

Som fællesoffentlig systemforvalter leverandørstyrer Databehandleren i forbindelse med levering af VDX til den Dataansvarlige.

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

I transmissionen i VDX behandles almindelige, fortrolige og følsomme personoplysninger, herunder helbredsoplysninger.

I VDX-API'et behandles almindelige personoplysninger i form af navn, organisatorisk tilhørsforhold, telefonnummer, arbejdsmail, logning af adfærd i VDX-API'et.

A.4. Behandlingen omfatter følgende kategorier af registrerede

I VDX behandles følgende kategorier af registrerede: Patienter, borgere, sundhedspersoner og administrativt personale.

I VDX-API'et behandles følgende kategorier af registrerede: Brugere i VDX-API'et – dvs. teknisk og administrativt personale hos den Dataansvarlige.

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

Databehandlingens varighed følger den indgåede tilslutningsaftale for VDX.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Udfyldes efter indgåelse af kontrakt			

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarliges skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

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

Databehandling	Beskrivelse af databehandling
Opbevaring	Hosting, drift, vedligehold, backup
Tilpasning eller ændring	Tilpasning eller ændring af personoplysninger i VDX-API'et på foranledning af den Dataansvarlige.
Brug	De almindelige personoplysninger i VDX-API'et bruges til support og udsendelse af servicemeddelelse om driften af VDX.
Videregivelse ved transmission	Hosting, drift, vedligehold
Sletning eller tilintetgørelse	Ved ophør af tilslutningsaftalen for VDX slettes personoplysningerne i VDX-API'et.
Leverandørstyring	Som fællesoffentlig systemforvalter leverandørstyrer Databehandleren i forbindelse med levering af VDX til den Dataansvarlige.
Support	De almindelige personoplysninger i VDX-API'et bruges til support.

C.2. Behandlingssikkerhed

1) Sikkerhedsniveauet skal afspejle, at der i VDX behandles følsomme og fortrolige personoplysninger, hvorfor der skal etableres et højt sikkerhedsniveau.

2) Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etableret det nødvendige (og aftalte) sikkerhedsniveau.

3) Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

C.2.1 Fastlæggelse af sikkerhedsniveau

1) Databehandleren skal have passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang. Databehandleren skal evaluere og forbedre effektiviteten af sådanne forholdsregler, når det er nødvendigt.

2) Databehandleren skal understøtte den Dataansvarlige i dennes arbejde med at dokumentere de identificerede risici og hvordan risikoen er nedbragt til et acceptabelt niveau

og gennemføre de foranstaltninger, der er nødvendige for at imødegå identificerede risici. Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:

a. Pseudonymisering og kryptering af personoplysninger
b. Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og – tjenester
c. Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
d. En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

3) Databehandling omfattet af Databehandleraftalen skal ske i overensstemmelse med denne instruks.

4) Denne instruks afspejler, hvad der er gældende på tidspunkt for underskrift af Databehandleraftalen. Såfremt der sker ændringer i forholdene, herunder i det af Databehandleren udfyldte, skal den Dataansvarlige orienteres.

5) Instruksen er en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Databehandleren minimum har ansvar for at gennemføre, overholde og sikre overholdelse af hos denne og dennes Underdatabehandlere. Eventuelle aftaler mellem den Dataansvarlige og Databehandleren om fravigelse eller delvis fravigelse af et eller flere af nedenstående krav dokumenteres i bilag D.

6) Såfremt mere omfattende tekniske og organisatoriske sikkerhedsforanstaltninger er nødvendige for at sikre efterlevelse af Databehandleraftalens punkt 5, skal sådanne foranstaltninger altid træffes. Supplerende sikringsforanstaltninger angives i bilag D.

7) Databehandleren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger og som dermed opfylder Databeskyttelsesforordningens artikel 32. Foranstaltningerne fastlægges ud fra overvejelser om:

a. Hvad der kan lade sig gøre rent teknisk
b. Implementeringsomkostningerne
c. Den pågældende behandlings karakter, omfang, sammenhæng og formål
d. Konsekvenserne for den registreredes rettigheder ved et sikkerhedsbrud
e. Den risiko, der er forbundet med behandlingerne

C.2.2 Pseudonymisering og kryptering

1) Videokommunikation mod VDX anvender internettet som transportvej. Kryptering af transmissionen i VDX sker med minimum TLS 1.3.

2) Videokommunikationen er krypteret på nær for faste videoanlæg hos de Dataansvarlige, som ikke tillader eller har slået kryptering fra. Den Dataansvarlige er her selv ansvarlig for at etablere den nødvendige sikkerhed.

3) E-mails indeholdende fortrolige og følsomme personoplysninger skal også være beskyttet af kryptering.

C.2.3 Sikring af fortrolighed integritet, tilgængelighed og robusthed af behandlingssystemer

1) Databehandleren skal have formelle procedurer til sikring af, at opdateringer til operativsystemer, databaser, applikationer og anden software bliver vurderet og implementeret inden for rimelig tid.

2) Databehandleren skal have formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering. Proceduren skal understøttes af en effektiv funktionsadskillelse eller ledelsesopfølgning med henblik på at sikre, at ingen enkeltpersoner kan implementere en ændring alene.

3) Databehandleren skal mindst en gang årligt gennemgå sine interne sikkerhedsforskrifter og retningslinjer for behandling af personoplysninger. Dette med henblik på at sikre, at de fornødne sikkerhedsforanstaltninger til stadighed iagttages.

4) Der stilles krav om, at alle ansatte hos Databehandleren modtager den tilstrækkelig uddannelse og instruktioner for at sikre, at personoplysninger behandles i overensstemmelse med relevant lovgivning samt Databehandlerens og den Dataansvarliges politikker og procedurer herfor.

C.2.4 Adgangsstyring- og kontrol

1) Der skal gennemføres styring af den generelle adgang til personoplysninger.

2) Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har brug for.

    a) Den Dataansvarlige er selv ansvarlig for autorisation, oprettelse, tildeling af rettigheder og kontrol af adgang for egne medarbejdere til VDX-API'et. VDX-API'et stiller information til rådighed for den Dataansvarlige for kontrol af anvendelsen af VDX-API'et.

    b) Databehandler og Underdatabehandler er hver især ansvarlige for autorisation, oprettelse, tildeling af rettigheder og kontrol af adgang for egne medarbejdere til VDX og VDX-API'et.

3) Der gennemføres begrænsninger i adgangen til systemer og personoplysninger, der behandles i henhold til Databehandleraftalen, ved at definere brugerroller, for så vidt det er muligt og ved at tildele privilegerede adgangsrettigheder samt at udføre attestering af brugere.

4) Databehandleren skal træffe foranstaltninger til at sikre, at kun autoriserede brugere kan få adgang til personoplysninger, som den pågældende er autoriseret til.

5) Der skal foreligge oversigt/dokumentation over de enkelte medarbejderes rettigheder til de individuelle systemer og personoplysninger, der behandles i henhold til Databehandleraftalen.

6) Der skal gøres brug af sikre adgangskoder/passwords og autentifikation – samt multifaktorautentifikation ved adgang fra det åbne internet – eller tilsvarende sikkerhedsniveau, ved adgang til systemer eller personoplysninger, der behandles i henhold til Databehandleraftalen.

7) Databehandleren skal have formelle procedurer for håndtering af nulstilling af adgangskoder og for andre situationer, hvor den normale logiske adgangskontrol sættes ud af kraft.

8) Der skal løbende foretages kontrol af, om brugerne er tildelt de adgange og autorisationer, som de bør have. Denne kontrol kan f.eks. indebære, at der i systemerne dannes en statistik over den enkelte brugers anvendelse af systemet, så det kan konstateres, om udstedte adgange og autorisationer fortsat anvendes.

9) Frekvens for kontrollen fastlægges på baggrund af risikovurderingen:

   a) Underdatabehandlerens autoriserede brugere gennemgås på fælles driftsmøder.

   b) Databehandler og Underdatabehandleren attesterer sine medarbejderes adgang hvert halve år.

10) Databehandleren skal uden unødig forsinkelse inddrage autorisationer og adgange for brugere, der efter en konkret vurdering ikke længere bør have disse.

11) Der skal foretages registrering af alle afviste adgangsforsøg, når der behandles fortrolige og/eller følsomme personoplysninger. Databehandleren skal løbende foretage opfølgning på afviste adgangsforsøg. Adgange blokeres efter 3 fejlede loginforsøg.

12) Ved genåbning af adgange, skal der foreligge dokumentation/en beskrivelse af på hvilken baggrund genåbning er sket, og om der sendes besked den Dataansvarlige ved blokeret adgangsforsøg.

13) Autoriserede personer skal kunne fremvise billed-ID ved on-site databehandling hos den Dataansvarlige.

14) Ved integration til egen brugerstyring er den tilsluttede part selv ansvarlig for krav til og de tekniske og organisatoriske foranstaltninger for adgangsstyring -og kontrol - fx multifaktor autentifikation, log over og kontrol med afviste adgangsforsøg

C.2.5 Genoprettelse af tilgængelighed i tilfælde af fysisk eller teknisk hændelse

1) Personoplysninger, der transmitteres i VDX, gemmes ikke. Der tages backup af VDX-API'et

2) Der gælder de samme retningslinjer for backup som for al anden behandling af personoplysninger, der behandles i henhold til Databehandleraftalen.

3) Databehandleren skal sikre, at der foretages regelmæssig backup af systemer og personoplysninger, der behandles i henhold til Databehandleraftalen.

4) Backuppen opbevares på en anden geografisk lokation for at sikre, at denne ikke går tabt. Backup skal beskyttes og opbevaring af backup skal altid ske på betryggende vis

så denne ikke fortabes. Den præcise adresse er af sikkerhedsmæssige grunde fortrolig, men kan på anmodning til vdx@medcom.dk oplyses.

5) Databehandleren skal regelmæssigt kontrollere, at backup er læsbart. Dette skal blandt andet gøres ud fra et beredskabssynspunkt, f.eks. ved større ændringer af et systems tekniske setup.

6) Databehandleren skal have dokumenterede it-beredskabsprocedurer, der sikrer genetablering af services inden for rimelig tid i tilfælde af driftsafbrydelser.

7) Databehandleren skal regelmæssigt afprøve og evaluere effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed gennem afholdelse af it-beredskabsøvelser. Den Dataansvarlige kan anmode om at få dokumentation for dette stillet til rådighed.

C.2.6 Adgang til oplysningerne via internettet

1) Der må kun etableres eksterne kommunikationsforbindelser, hvis forbindelsen er krypteret f.eks. til webside, front-ends og loginportaler. Dette gælder også forbindelser til underleverandøren f.eks. site-to-site forbindelse eller IP-filtrering. Ved fortrolige og følsomme personoplysninger forventes der en stærk kryptering. HTTPS og nyest mulige version af TLS er et krav.

2) Kryptering af forbindelse til VDX-API'et sker med minimum TLS 1.3.

3) Der skal gøres brug af sikre adgangskoder/passwords og autentifikation – samt multifaktorautentifikation ved adgang fra det åbne internet – eller tilsvarende sikkerhedsniveau, ved adgang til systemer eller personoplysninger, der behandles i henhold til Databehandleraftalen.

4)

C.2.7 Beskyttelse af oplysninger under transmission

1) Videokommunikation mod VDX anvender internettet som transportvej. Kryptering af transmissionen i VDX sker med minimum TLS 1.3.

2) Videokommunikationen er krypteret på nær for faste videoanlæg hos de Dataansvarlige, som ikke tillader eller har slået kryptering fra. Den Dataansvarlige er her selv ansvarlig for at etablere den nødvendige sikkerhed.

3) E-mails indeholdende fortrolige og følsomme personoplysninger skal også være beskyttet af kryptering.

C. 2.8 Fysisk sikring af lokaliteter, hvor der behandles oplysninger

1) Databehandleren skal sikre, at it-udstyr, der anvendes i forbindelse med databehandlingen, er fysisk sikret i henhold til gældende lovkrav.

2) Databehandleren skal have passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang. Databehandleren skal desuden evaluere og forbedre effektiviteten af sådanne forholdsregler, hvor det er nødvendigt.

3) Mobile lagringsmedier med personoplysninger skal være mærket og skal opbevares med tilstrækkelig stærk kryptering under opsyn eller under lås, når de ikke benyttes.

4) Mobile lagringsmedier med personoplysninger må kun udleveres til autoriserede personer med henblik på revision eller drifts- og systemtekniske opgaver.

5) Der skal føres en fortegnelse over, hvilke mobile lagringsmedier der benyttes i forbindelse med databehandlingen.

6) Der skal udarbejdes skriftlige instrukser for anvendelse og opbevaring af mobile lagringsmedier.

7) I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier skal der træffes fornødne foranstaltninger for at sikre, at personoplysningerne ikke hændeligt eller bevidst tilintetgøres, fortabes eller forringes eller, at personoplysningerne kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med gældende lov. Dette skal ske efter best-practice.

8) Ved kassation af udstyr og lagringsmedier, der indeholder personoplysninger, skal lagringsmedier destrueres eller afmagnetiseres, så der sker effektiv sletning af personoplysningerne. Dokumentation for, at kassation er foretaget i overensstemmelse med ovenstående, skal opbevares i den periode, databehandlingen foregår og forevises, når den Dataansvarlige anmoder herom

C.2.9 Anvendelse af hjemme/fjernarbejdspladser

1) Databehandleren og dennes autoriserede medarbejdere må foretage databehandling fra mobile arbejdspladser, herunder med adgange til den Dataansvarliges personoplysninger over internettet, såfremt databehandlingen sker fra arbejdspladser, som er underlagt Databehandlerens egne sikkerhedsregler. Databehandlingen skal endvidere ske i overensstemmelse med Databehandleraftalen og denne instruks.

2) Hjemme-/Ad hoc-arbejdspladserne skal være sikret med tekniske kontroller, der sikrer, at behandlingen af personoplysninger sker i overensstemmelse med gældende lovgivning og den Dataansvarliges og Databehandlerens retningslinjer.

3) Det skal sikres, at uvedkommende ikke får adgang til personoplysninger, der behandles ved hjemmearbejdspladser, ligesom de enkelte medarbejdere skal instrueres i, hvordan uvedkommende ikke får adgang.

4) Fjernadgang til VDX sker via minimum AES256-bit-krypteret VPN-adgang med multifaktor-autentifikation.

C.2.10 Logning

1) Der skal som udgangspunkt foretages maskinel registrering (logning) ved behandling af personoplysninger. Krav til logning og indhold af loggen fastlægges på baggrund af risikovurderingen samt eventuelle lovkrav og omfang af den aftalte logning.

2) Loggen skal opbevares i den periode, der aftales mellem den Dataansvarlige og Databehandleren under hensyn til eventuelle lovkrav.

3) Brugerhandlinger i VDX-API'et dokumenteres i en hændelseslog, som slettes efter 2 år. Loggen er tilgængelig for den Dataansvarlige for opfølgning på egne autoriserede medarbejderes handlinger jf. egne politikker.

4) Databehandleren har gennem Underdatabehandlere etableret logning på alt aktivt netværksudstyr i VDX. Logningen omfatter en log over anvendelsen af privilegerede konti på aktivt netværksudstyr, herunder navn, start og sluttidspunkt samt formålet med brugen af den privilegerede konto.

5) Underdatabehandleren foretager overvågning af og reagerer på uautoriserede forespørgsler i loggen - samt foretager overvågning af loggen i forhold til identificering af misbrug af VDX.

6) Underdatabehandleren opbevarer transaktionsloggen på Underdatabehandlerens adgang til VDX i 2 år.

7) Driftslog uden personoplysninger opbevares i 5 år til brug ved opfølgning/undersøgelse af evt. ulovlige eller kriminelle handlinger.

8) Alle logs er beskyttet mod uautoriseret adgang, manipulation og tekniske fejl**.**

C.2.11 Tilsyn

Databehandleren skal føre og dokumentere et tilsyn med Databehandlerens organisations overholdelse af lovkrav, politikker, procedurer og denne Databehandleraftale med bilag.

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:

Databehandleren opretholder i sin interne organisation passende politikker og procedurer, som understøtter, at Databehandleren er i stand til at leve op til sine forpligtelser som Databehandler, herunder ift. at kunne bistå den Dataansvarlige på en måde som understøtter den Dataansvarliges iagttagelse af de frister, som følger af gældende databeskyttelsesretlig lovgivning.

C.4 Opbevaringsperiode/sletterutine

1) Personoplysninger opbevares, så længe opbevaringen er nødvendig til opfyldelse af databehandlingens formål.

2) Personoplysninger i transmissionen i VDX gemmes ikke.

3) Personoplysninger i VDX-API'et oprettes og slettes af den Dataansvarlige selv.

4) Ved ophør af tilslutning til VDX, sletter Databehandler personoplysningerne om den Dataansvarlige i VDX-API'et. Personoplysningerne vil fortsat fremgå af hændelsesloggen, som slettes efter 2 år.

5) Log fra den underliggende netværksinfrastruktur i VDX, som alene indeholder persondata om Databehandlerens og evt. Underdatabehandlerens medarbejdere, skal opbevares i 2 år til brug ved opfølgning/undersøgelse af evt. ulovlige eller kriminelle handlinger.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal Databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med Bestemmelse 10.1, medmindre den Dataansvarlige – efter underskriften af disse Bestemmelser – har ændret den Dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til Bestemmelserne.

C.5 Lokalitet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

Virksomhed	**Rolle (Databehandler/Underdatabehandler)**	**Adresse**	**Type af behandling, virksomheden foretager**
Udfyldes med ny kontrakt	*Udfyldes med ny kontrakt*	*Udfyldes med ny kontrakt*	*Udfyldes med ny kontrakt*

Data behandles på lokationer på servere beliggende inden for EU/EØS.

De præcise adresser er af sikkerhedsmæssige grunde fortrolige, men kan på anmodning oplyses. Medcom kan kontaktes for nærmere oplysninger på vdx@medcom.dk.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

1) VDX kan levere tilslutning af udenlandske parter, herunder i usikre tredjelande.

2) Transmissionen af personoplysninger til en udenlandske part forudsætter instruks fra den Dataansvarlige i form af booking af videomøde. Det påhviler den Dataansvarlige at sikre, at der er et lovligt grundlag for overførsel af personoplysninger til usikre tredjelande.

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.

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

1) Den Dataansvarliges tilsyn med Databehandleren fastlægges ud fra en risikovurdering. I vurderingen af tilsynsformen skal der tages hensyn til omfanget af personoplysninger og deres følsomhed, evt. lovgivningsmæssige krav samt hvor kritisk databehandlingen er for organisationens opgaveløsning.

2) Databehandleren vil årligt på eget initiativ og regning få gennemført en ISAE3000-erklæring af uafhængig revisor for at kunne dokumentere overholdelse af Databeskyttelsesloven og GDPR. Erklæringen dokumenterer desuden overholdelse af udvalgte relevante sikkerhedskrav til VDX. Erklæringen er møntet på det specifikke forhold mellem Databehandleren og den Dataansvarlige. Erklæringen fremsendes til den Dataansvarlige.

3) Baseret på resultatet af tilsynet skal Databehandleren iværksætte evt. yderligere foranstaltninger, hvis dette er nødvendigt for at efterleve kravene i denne databehandleraftale.

4) Det er den Dataansvarliges ansvar at vurdere, om erklæringen er tilstrækkelig til at opfylde den Dataansvarliges tilsynsbehov.

5) Databehandleren er forpligtet til at føre tilsyn med evt. Underdatabehandlere. Databehandleren vil årligt og på eget initiativ indhente og behandle erklæringer fra Underdatabehandlere. Efter anmodning fra den Dataansvarlige skal dokumentation for tilsynet fremsendes til den Dataansvarlige.

6) Den Dataansvarlige skal selv afholde omkostningerne ved yderligere auditering, herunder Underdatabehandleres medvirken – med undtagelse af, hvis en auditering kommer på baggrund af brud på persondatasikkerheden, anmærkninger i revisionserklæringer eller andre objektivt konstaterbare forhold.

7) Den Dataansvarlige kan beslutte, at der som supplement skal være adgang for den Dataansvarlige eller en repræsentant at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra Databehandleren eller evt. Underdatabehandlere foretager behandling af personoplysninger.

Bilag D Parternes regulering af andre forhold

D1 Governance

Kravene til VDX fastsættes af MedComs styregruppe, og Dataansvarlig kan ikke selvstændigt stille krav til VDX. Hvis Dataansvarlig kræver specifikke foranstaltninger implementeret i VDX, uden at tilsvarende krav er vedtaget af MedComs styregruppe, skal sådanne foranstaltninger alene kunne implementeres på den dataansvarliges regning.

I det omfang flere Dataansvarlige kræver de samme foranstaltninger, kan de pågældende Dataansvarlige dele omkostningerne til foranstaltningerne.

Sikkerhedspolitik mv. for VDX kan til enhver tid rekvireres hos MedCom.

D2 Sikkerhedsgodkendelse af medarbejdere

Den Dataansvarlige vil kunne kræve sikkerhedsgodkendelser af medarbejdere hos Databehandleren eller dennes Underdatabehandlere. Databehandleren eller dennes Underdatabehandlere skal stille sig til rådighed herfor.

Eventuelle udgifter hertil vil skulle afholdes af den Dataansvarlige.

D3 Pligt til at informere den anden part

Databehandleren skal:

a) Informere den Dataansvarlige uden unødigt ophold om overvågnings-aktiviteter og foranstaltninger iværksat overfor Databehandleren vedrørende oplysninger behandlet på vegne af den Dataansvarlige i henhold til gældende lovgivning medmindre sådan lovgivning forbyder Databehandleren at informere den Dataansvarlige.
b) Informere den Dataansvarlige, såfremt en registreret anlægger retssag mod Databehandleren, jf. databeskyttelsesforordningens artikel 79.

Den Dataansvarlige skal:

c) Informere Databehandleren uden unødigt ophold, hvis den Dataansvarlige bliver opmærksom på et brud på persondatasikkerheden, som Databehandleren potentielt har en rolle i.
d) Informere Databehandleren, såfremt en registreret anlægger retssag mod Databehandleren, jf. databeskyttelsesforordningens artikel 79.

D4 Lovvalg og værneting

Enhver tvist og ethvert krav, som måtte udspringe af disse Bestemmelser skal afgøres i overensstemmelse med bestemmelser om lovvalg og værneting i tilslutningsaftalen for VDX.

D5 Erstatningsansvar

Tilslutningsaftalens regulering om begrænsning af erstatningsansvar og skadesløsholdelse finder anvendelse på disse Bestemmelser - og intet i disse Bestemmelser skal tolkes som en udvidelse af erstatningsansvaret og skadesløsholdelsespligterne i tilslutningsaftalen for VDX.

Databehandlerens ansvar efter databeskyttelsesforordningens artikel 82 over for den Dataansvarliges eventuelle regreskrav, er tilsvarende begrænset i overensstemmelse med Tilslutningsaftalens regulering om skadesløsholdelse og begrænsning af ansvar.

D6 Regulering fra tilslutningsaftalen for VDX efter tilslutningsaftalens ophør

Hvis tilslutningsaftalen for VDX ophører før disse Bestemmelser, skal de følgende reguleringstemaer fra tilslutningsaftalen fortsat være gældende i relation til disse Bestemmelser, så længe Bestemmelserne gælder:

- Erstatningsansvar og begrænsning heraf
- Tilsyn/kontrol og compliance
- Økonomisk regulering, herunder ift. priser
- Roller og ansvar i relation til tredjeparter
- Fortrolighed
- Lovvalg og værneting
- Opsigelse og ophør

D7 Særligt vedrørende backups

Efter, at der er sket sletning i VDX-API'et i overensstemmelse med Kontrakten og punkt 10 i Bestemmelserne, vil sletning i backups ske ved udløbet af den fastsatte retention-periode for den pågældende backup. Denne vil fremgå af driftshåndbogen.

D8 Sikker konfiguration og beskyttelse mod malware

Databehandleren sikrer gennem Underdatabehandler vedligeholdelse af software/firmware og konfigurationer - samt i relevant omfang vedligeholdelse af anti-malware og antivirus.

D9 Netværkssikkerhed

Der anvendes IDS/IPS-funktionalitet i VDX, og der gennemføres månedlige sårbarhedsskanninger samt ved større ændringer.

D10 Overvågning

Databehandleren overvåger VDX gennem Underdatabehandleren, så Underdatabehandleren kan reagere på og forhindre afbrydelser, på baggrund af overskridelse af grænseværdier.

D11 Ændringer

Genforhandling af vilkårene i Databehandleraftalen sker i den governance, der er aftalt for VDX.