Standardkontraktsbestemmelser

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

mellem

Kunde
CVR XXX
Adresse

herefter ”den dataansvarlige”

og

Fischer & Kerrn A/S
CVR 24237087
Amagerfælledvej 106
2300 København S
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 softwaresystemet CONCIERGE BOOKING 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.

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.

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

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 specifik skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse på mindst 30 dage inden anvendelsen af den

pågældende underdatabehandler. 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 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 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 4 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
   Stilling
   Telefonnummer
   E-mail
   Underskrift

   På vegne af databehandleren

Navn	Henrik Fehrn
Stilling	CEO
Telefonnummer	+45 25 60 09 33
E-mail	hfe@fischerkerrn.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.

   På vegne af den dataansvarlige

   Navn
   Stilling
   Telefonnummer
   E-mail

   På vegne af databehandleren

Navn	Henrik Fehrn
Stilling	CEO
Telefonnummer	+45 25600933
E-mail	hfe@fischerkerrn.dk

Bilag A Oplysninger om behandlingen

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

Fischer & Kerrn behandler personoplysninger på vegne af den dataansvarlige med det formål at tilbyde software til registrering og behandling af møder, gæster og vare-/tjenestebestillinger.

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

Fischer & Kerrn indsamler og opbevarer personoplysninger på vegne af den dataansvarlige for at den dataansvarlige er i stand til at:

- orientere mødedeltagere/gæster omkring kommende møder/besøg
- effektivt at planlægge bookningen af den dataansvarliges ressourcer (lokaler, udstyr, mv).
- udtrække historik over hvilke mødedeltagere/gæster, der har besøgt den dataansvarliges lokationer
- foretage afregning af bestilte varer/tjenester til rette vedkommende

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

Følgende personoplysninger indsamles og opbevares:

- Navn
- Email
- Telefon
- Ansættelsessted (firma)

Følgende oplysninger, der kan have særlig interesse og som potentielt kan relateres til personer, indsamles og opbevares:

- Bestilte varer/tjenester/ressourcer
- Kommentarer til bestillinger omkring allergier, præferencer osv.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Følgende kategorier af registrerede er omfattet af behandlingen:

- Medarbejdere
- Forretningsforbindelser og gæster, herunder kunder, leverandører og samarbejdspartnere

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

A.5.1. Denne Aftale træder i kraft ved begge Parters underskrift heraf.

A.5.2. Medmindre andet skriftligt aftales, forbliver aftalen i kraft så længe databehandleren behandler data på vegne af den Dataansvarlige eller frem til aftalens ophør (det seneste tidspunkt af de to begivenheder).

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Microsoft West Europe Netherlands		Evert van de Beekstraat 354, 1118 CZ Luchthaven Schiphol, Noord-Holland, Netherlands	Datacenter placeret i Holland

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.

B.2. Varsel for godkendelse af underdatabehandlere

Ikke relevant

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:

- Indsamler personoplysninger om medarbejdere, forretningsforbindelser og gæster.
- Opbevarer personoplysninger om medarbejdere, forretningsforbindelser og gæster, så længe den dataansvarlige finder det relevant i forhold til ønsker om statistik og rapporteringsmuligheder
- Stiller personoplysninger til rådighed for den dataansvarlige i forbindelse med dennes rapportering og behandling af personoplysningerne.
- Sletter personoplysninger på foranledning af den dataansvarlige.

C.2. Behandlingssikkerhed

Den generelle behandlingssikkerhed for at undgå at oplysninger ikke hændeligt eller ulovligt tilintetgøres, fortabes, forringes, kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med de til enhver tid gældende regler og forskrifter for behandling af personoplysninger opretholdes gennem databehandlerens organisatoriske, administrative og IT-sikkerhedsmæssige foranstaltninger.

Databehandleren fastsætter for alle behandlinger sikkerhedsniveauet efter det højeste niveau hos Databehandleren.

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

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

C.2.1. Adgangsstyring og Autorisation

- Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.
- Der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger samt procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov.
- Når det arbejdsbetingede behov ikke længere er til stede lukkes brugernes adgang.

C.2.2. Opretholdelse af sikkerhedsforanstaltninger

- Data opbevares i Azure Datacenter og kan kun tilgås af udvalgte medarbejdere og kun såfremt der er et egentlig driftsbehov for dette. Udgangspunktet er at adgang til data ikke er mulig andet end via softwaren som også kører i Azure Datacenter og at der derfor efter behov fx pga. support eller driftsproblemer skal åbnes op for adgangen. Det logges når der åbnes op for denne adgang.

- Fjernadgang til maskiner hvor softwaren afvikles i Azure Datacenter er kun muligt for udvalgte medarbejdere, kun fra Fischer & Kerrns arbejdsnetværk (via IP-begrænsning) og kun når der åbnet op for denne adgang.
- Kunders data ligger i forskellige databaser og en given kundes instans af softwaren kører isoleret fra andres kunders instanser af softwaren. Der er dermed ingen software-processer og/eller databaser, der behandler eller opbevarer data fra flere kunder samtidigt.
- De indførte tekniske og organisatoriske sikkerhedsforanstaltninger er til enhver tid beskrevet på Databehandlerens hjemmeside for de relevante systemer.
- De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests. Disse foretages af den dataansvarlige.

C.2.2.1. Instruktion af medarbejdere

- Databehandleren instruerer de relevante medarbejdere om databehandlingens formål og arbejdsgange.

C.2.2.2. Tavshedspligt

- Databehandlerens medarbejderne er underlagt tavshedspligt under og efter deres ansættelse ved databehandleren.

C.2.2.3. Fysisk sikring

- Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler, hvori der opbevares og behandles personoplysninger.

C.2.2.4. Netværks- og kommunikationssikkerhed

- Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.
- Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.
- Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.
- Netværkstrafikken overvåges.

C.2.2.5. Driftsprocedurer og ansvarsområder

- Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.
- Der er etableret logning i systemer, databaser og netværk af følgende forhold:
    - Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder.
    - Sikkerhedshændelser omfattende:
        - Ændringer i logopsætninger, herunder deaktivering af logning.
        - Ændringer i systemrettigheder til brugere.
        - Fejlede forsøg på log-on til systemer, databaser og netværk.
- Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.

- Data og konfiguration bliver løbende (i realtid) duplikeret til flere servere, således at data til enhver tid eksisterer i mindst tre kopier.
- Sikkerhedskopiering af data og konfiguration kan foretages for at sikre mod katastrofescenarier hvor alle realtids-kopier af data mistes. Frekvensen for en sådan sikkerhedskopiering sker efter nærmere aftale med kunden idet frekvensen fastlægges efter hvor lang tids datatab der er acceptabelt. Test af genskabelse af data fra sikkerhedskopi i tilfælde af et katastrofescenarie sker ligeledes efter nærmere aftale med kunden og frekvensen fastlægges også her efter hvor lang tids datatab der er acceptabelt.
- Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i anonymiseret form.
- Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.
- Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.

C.2.2.6. Katastrofeplan

- Beskrivelsen i C.2.2.5 beskriver hvordan systemet kan genskabes efter at have været utilgængeligt i en periode.

C.3 Bistand til den dataansvarlige

Databehandleren sikrer, at databehandlerens systemer og interne processer er indrettet på en sådan måde, der gør det muligt for databehandleren at bistå den dataansvarlige med at varetage de registreredes rettigheder i tilfælde, hvor den dataansvarlige ikke er i stand til at gøre dette uden databehandlerens medvirken samt i tilfælde, hvor databehandleren på forhånd er blevet instrueret i at varetage en eller flere af de registreredes rettigheder på vegne af den dataansvarlige.

Databehandleren vil i de tilfælde, hvor det er muligt og relevant i forhold til den pågældende behandling, sørge for, at databehandlerens systemer er indrettet på en måde, som gør det muligt for den dataansvarlige selv at varetage de registreredes rettigheder direkte i databehandlerens systemer således, at databehandlerens bistand ikke vil være påkrævet.

Modtager databehandleren en henvendelse fra en registreret, hvis personoplysninger databehandleren behandler på vegne af den dataansvarlige, tager databehandleren kontakt til den dataansvarlige for at blive instrueret i, hvordan en sådan henvendelse skal håndteres, medmindre databehandleren på forhånd er blevet instrueret i at varetage en sådan henvendelse. En sådan instruks skal fremgå af dette afsnit.

C.3.1. Bistand til foretagelse af en konsekvensanalyse

Databehandlerens systemer og interne processer er indrettet på en sådan måde, at databehandleren, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, kan bistå den dataansvarlige med dennes forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse), samt bistå den dataansvarlige med dennes forpligtelse til at høre Datatilsynet inden behandling, såfremt konsekvensanalysen viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

C.3.2. Bistand til anmeldelse af brud til tilsynsmyndigheden og underretning af de registrerede
Databehandlerens systemer og interne processer er indrettet på en sådan måde, at databehandleren uden unødig forsinkelse, og senest 4 timer efter, at denne er blevet bekendt med bruddet, kan underrette den dataansvarlige om brud på persondatasikkerheden. Databehandleren bistår, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med de nødvendige oplysninger om bruddet således, at den dataansvarlige kan opfylde sin forpligtelse til uden unødig forsinkelse, og om muligt senest 72 timer efter, at denne er blevet bekendt med det at anmelde brud på persondatasikkerheden.

Oplysningerne om bruddet fremsendes til den dataansvarliges kontaktperson via e-mail og følges op at et telefonopkald.

Databehandlerens systemer og interne processer er ligeledes indrettet på en sådan måde, at databehandleren kan stille de nødvendige oplysninger til rådighed for den dataansvarlige, så den dataansvarlige kan vurdere, hvorvidt de registrerede skal underrettes om brud på persondatasikkerheden. Vurderer den dataansvarlige herefter, at der skal foretages underretning af de registrerede, bistår databehandleren, efter anmodning fra den dataansvarlige, med at foretage en sådan underretningen i tilfælde, hvor underretning ikke kan ske uden databehandlerens medvirken.

C.4 Opbevaringsperiode/sletterutine
Personoplysninger vil af databehandleren blive slettet i henhold til slettepolitikken, som den dataansvarlige udleverer (hvor personoplysningerne automatisk slettes af databehandleren i overensstemmelse hermed), i det omfang, data opbevares af databehandleren.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, 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:

Fischer & Kerrn, DK
Microsoft, Datacenter i Holland

C.6 Instruks vedrørende overførsel af personoplysninger til 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

Der er i Databehandleraften aftalt følgende tilsyn: Databehandleren forpligter sig til årligt at give en skriftlig status på forhold, der er omfattet af databehandleraftalen. Statusrapporteringen kan foregå ved, at Databehandleren deler oplysningerne via sin hjemmeside, eller ved at oplysningerne deles direkte med den Dataansvarlige. Statusrapporteringen skal give den Dataansvarlige en tilstrækkelig mulighed for at vurdere om betingelserne i databehandleraftalen fortsat overholdes. Den Dataansvarlige kan på baggrund af den udarbejdede status gebyrfrit anmode om præciseringer eller yderligere oplysninger i relation til det materiale, der er blevet stillet til rådighed.

Den Dataansvarlige har ret til en gang årligt med et passende skriftligt varsel og mod afholdelse af omkostningerne dertil at udføre undersøgelse af eller lade en uafhængig ekspert udføre undersøgelse af, hvorvidt Databehandleren har truffet de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger i forhold til behandlingen af de personoplysninger, som er omfattet af disse Bestemmelser.

Eksperten skal behandle enhver information indhentet hos eller modtaget fra Databehandleren fortroligt og må kun udlevere sine konklusioner til den Dataansvarlige. Databehandleren skal modtage en kopi af ekspertens rapport og være berettiget til at anvende denne som dokumentation overfor andre kunder i relevant omfang.

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

Den Dataansvarlige kan ligeledes bede om en kopi af passende revisionserklæring fra Databehandlerens eventuelle underdatabehandlere. Såfremt det ikke giver mening at lave en selvstændig revisionserklæring vedrørende en underdatabehandler, eksempelvis fordi den ydelse, underdatabehandleren leverer, er af begrænset omfang eller ikke frembyder selvstændige problemstillinger, fordi underdatabehandleren kun behandler data i Databehandlerens egne systemer, kan Databehandleren opfylde kravet i denne bestemmelse med en erklæring som Databehandleren selv udarbejder. Erklæringen vil bestå i en redegørelse for underdatabehandlerens rolle og en overordnet redegørelse for sikkerheden i relation til underdatabehandlerens virke samt en indeståelse for, at underdatabehandleren er underlagt og opfylder de samme krav, som der stilles til Databehandleren efter disse Bestemmelser.