Bilag A – Oplysninger om behandlingen

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

Parterne har aftalt, at databehandleren skal levere følgende ydelser:

Valgt (X)	Behandlingsaktiviteter
☒	Hosting og drift Angivet som Services i kategorierne Backup & Restore, Datacenter, Server Operation, Network og Workplace i bilag "Leverandørens Services" i parternes aftale vedrørende levering af Services.
☒	Support
☒	Konsulentydelser
☒	Databaseadministration
☒	Konfiguration og udvikling
☒	Drift og service af applikationsservices
☒	Sikkerhedsservices

A.1.1 Hosting og drift

Såfremt Hosting og drift er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Formålet med behandlingen er levering af hosting og drift af den dataansvarliges IT-systemer herunder backup, overvågning, vedligehold og support som nærmere specificeret i aftalen vedrørende levering af Services indgået mellem parterne. Herunder også specifikke opgaver bestilt af den dataansvarlige.

A.1.2 Support

Såfremt support er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Formålet med behandlingen er levering af supportydelser til den dataansvarlige som nærmere specificeret i Serviceaftalen indgået mellem parterne. Herunder også specifikke opgaver bestilt af den dataansvarlige.

A.1.3 Konsulentydelser

Såfremt konsulentydelser er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Formålet med behandlingen er at udføre specifikt aftalte konsulentopgaver. Formålet vil derfor variere, men altid have en sammenhæng til en aftalt konsulentopgave.

A.1.4 Databaseadministration

Såfremt databaseadministration er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Formålet med behandlingen er at udføre administrations opgaver på den dataansvarliges databaser og database servere, herunder administration af tabeller, jobs, performance optimering, backup, database storage, konfiguration og lignende opgaver, som nærmere specificeret i Serviceaftalen indgået mellem parterne. Herunder udføres også specifikke opgaver bestilt af den dataansvarlige.

A.1.5 Konfiguration og udvikling

Såfremt konfiguration og udvikling er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Formålet med behandlingen er at udføre specifikt aftalte udviklings- og konfigurationsopgaver på den dataansvarliges IT-systemer og applikationer.

A.1.6 Drift og service af applikationsservices

Såfremt drift og service af applikationsservices er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Formålet med behandlingen er levering af de i hovedaftalen aftalte applikationsservices til den dataansvarlige. Leveringen omfatter f.eks. implementering, drift, udvikling og support af de valgte applikationsservices, som nærmere specificeret i Servicesaftalen indgået mellem parterne.

A.1.7 Sikkerhedsservices

Såfremt sikkerhedsservices er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Formålet med behandlingen er levering af sikkerhedsservice til den dataansvarlige. Leveringen omfatter f.eks. managed eller unmanaged Security Information and Event Management (SIEM), penetrations test eller incident management efter et sikkerhedsbrud.

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

A.2.1 Hosting og drift

Såfremt hosting og drift er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Databehandleren yder hosting og drift af den dataansvarliges IT-systemer. Det primære formål med behandlingen udgør derfor hosting, herunder opbevaring af den dataansvarliges personoplysninger, og løbende drift, herunder overvågning, backup og vedligehold af den dataansvarliges IT-systemer indeholdende personoplysninger.

Behandlingen kan i de konkrete tilfælde blandt andet omfatte organisering, systematisering, facilitering, midlertidig opbevaring, filtrering, fejlfinding, tilpasning eller ændring, genfinding, søgning, brug, sammenstilling, samkøring, begrænsning eller sletning af personoplysninger, når det er nødvendigt i forbindelse med opfyldelse af databehandlerens levering af Services til den dataansvarlige, eller når det er nødvendigt for at opfylde en konkret anmodning fra den dataansvarlige.

A.2.2 Support

Såfremt support er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Databehandleren yder support til den dataansvarliges ansatte etc. Alt arbejde, som databehandleren yder som en del af supporten, og som omfatter behandling af personoplysninger på vegne af den dataansvarlige, foregår på den dataansvarliges specifikke anmodning.

Databehandleren supporterer den dataansvarlige med den dataansvarliges daglige drift af dennes IT-systemer. Databehandleren kan på den dataansvarliges opfordring overtage den dataansvarliges håndtering af den dataansvarliges IT-systemer på deres arbejdsplads eller servere via TeamViewer eller Remote Desktop til en konkret opgave. Derudover kan databehandleren tilgå systemer til håndtering af fejlsøgning og driftsopgaver.

Ved fejl i software eller den dataansvarliges IT-systemer i øvrigt kan databehandleren hente database fra den dataansvarlige med henblik på fejlsøgning, rettelser mv. Dette sker kun efter forudgående specifik aftale.

Behandlingen kan i de konkrete tilfælde blandt andet omfatte organisering, systematisering, facilitering, midlertidig opbevaring, filtrering, fejlfinding, tilpasning eller ændring, genfinding, søgning, brug, sammenstilling, samkøring, begrænsning eller sletning af personoplysninger, når det er nødvendigt i forbindelse med leveringen af de aftalte tjenester, eller når det er nødvendigt for at opfylde en anmodning fra den dataansvarlige.

A.2.3 Konsulentydelser

Såfremt konsulentydelser er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Databehandleren udfører opgaver i forbindelse med specifikke og afgrænsede opgaver. Konsulentopgaverne udføres på den dataansvarliges systemer og data, og behandlingen vil være defineret i den konkrete opgave.

Opgaverne bestilles og defineres af dataansvarlig, og databehandleren indgår i nødvendigt omfang i at sikre korrekt opgavedefinition.

A.2.4 Databaseadministration

Såfremt databaseadministration er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Databehandleren yder administration af den dataansvarliges databaser og database servere. Det primære formål med behandlingen udgør derfor administration, optimering, vedligehold, overvågning og fejlsøgning på dataansvarliges databaser indeholdende personoplysninger.

Behandlingen har ikke til primært formål at behandle persondata, men i forbindelse med udførelse af databehandlerens forpligtelser, kan der forekomme databehandling i den dataansvarliges databaser. Dette kan blandt andet omfatte organisering, midlertidig opbevaring, filtrering, fejlfinding, tilpasning eller ændring, genfinding, søgning, samkøring, eller sletning af personoplysninger, når det er nødvendigt i

forbindelse med opfyldelse af databehandlerens levering af Services til den dataansvarlige, eller når det er nødvendigt for at opfylde en konkret anmodning fra den dataansvarlige.

A.2.5 Konfiguration og udvikling

Såfremt konfiguration og udvikling er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Databehandleren udfører opgaver relateret til udvikling og konfiguration af den dataansvarliges forretningsapplikationer. Herunder udvikling af komponenter til ERP-systemer, CRM, SharePoint og andre applikationer. Opgaverne udføres efter specifik aftale med den dataansvarlige.

A.2.6 Drift og service af følgende applikationsservices

Såfremt drift og service af følgende applikationsservices er valgt som ydelse i skemaet i bilag A.1. gælder følgende:

Databehandleren yder vedligeholdelse, konfigurering, opdateringer, udvikling, support, hosting og drift af de valgte applikationsservices til den dataansvarlige, som er nærmere specificeret i Servicesaftalen indgået mellem parterne.

A.2.7 Sikkerhedsservices

Såfremt sikkerhedsservices er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Databehandleren udfører overvågning, opsætning, rapportering, penetrations test, incident management efter sikkerhedsbrud, som er nærmere specificeret i Servicesaftalen indgået mellem parterne.

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

Almindelige personoplysninger (jf. Databeskyttelsesforordningens artikel 6):

☒ Navn

☒ Adresse

☒ E-mail

☒ Telefonnummer

☒ Finansielle oplysninger

Følsomme personoplysninger (jf. Databeskyttelsesforordningens artikel 9):

☒ Racemæssig eller etnisk baggrund.

☒ Politisk overbevisning.

☒ Religiøs overbevisning.

☒ Filosofisk overbevisning.

☒ Fagforeningsmæssige tilhørsforhold.

☒ Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol m.v.

☒ Seksuelle forhold.

Oplysninger om enkeltpersoners rent private forhold (jf. Databeskyttelseslovens § 8):

☒ Strafbare forhold.

☒ Væsentlige sociale problemer.

Andre rent private forhold, som ikke er nævnt ovenfor:

☒ Andre private forhold.

Oplysninger om CPR-nummer (jf. Databeskyttelseslovens § 11):

☒ CPR-numre.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Kategorier af registrerede, identificerede eller identificerbare fysiske personer, som databehandlerens behandlinger vedrører:

☒ Ansatte

☒ Børn

☒ Den dataansvarliges egne kunder

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

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige påbegyndes, efter parternes aftale vedrørende levering af Services træder i kraft, og indtil denne ophører.

Bilag B – Underdatabehandlere

B.1. Godkendte underdatabehandlere

De til enhver tid anvendte underdatabehandlere fremgår af databehandlerens gældende oversigt over underdatabehandlere, som er tilgængelig på databehandlerens Legal landing page https://legal.itm8.com. Oversigten udgør den samlede og opdaterede liste over de underdatabehandlere, som den dataansvarlige har godkendt efter disse Bestemmelser. Databehandleren er berettiget til løbende at tilføje, erstatte og fjerne underdatabehandlere, forudsat at den dataansvarlige orienteres i overensstemmelse med Bestemmelserne i databehandleraftalen

Databehandlerens meddelelse om planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere sker som beskrevet i B.2.

B.2. Varsel for godkendelse af underdatabehandlere

Databehandlerens underretning om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere skal være den dataansvarlige i hænde minimum 30 dage, før anvendelsen eller ændringen skal træde i kraft, så vidt dette umiddelbart er muligt.

Uanset ovenstående accepterer den dataansvarlige, at der kan være særlige tilfælde, hvor der kan opstå et konkret behov for, at ændringen vedrørende tilføjelse eller erstatning af underdatabehandlere sker med kortere varsel eller straks. I sådanne tilfælde vil databehandleren underrette den dataansvarlige om ændringen snarest muligt. Særlige tilfælde kan være, men er ikke begrænset til følgende situationer:

- Hvor underdatabehandleren ikke kan levere den aftalte ydelse på grund af dennes konkurs, eller
- Tilfælde hvor underdatabehandleren misligholder kontrakten, eller
- Hvor ændringer i lov eller praksis umiddelbart forhindrer brugen af den pågældende
- underdatabehandler.

Såfremt den dataansvarlige har indsigelser mod ændringerne, skal den dataansvarlige give databehandleren meddelelse herom inden ændringens varslede virkningstidspunkt. Den dataansvarlige kan alene gøre indsigelse, hvis den dataansvarlige har rimelige, konkrete årsager hertil.

Ved den dataansvarliges indsigelse accepterer den dataansvarlige samtidig, at databehandleren kan være forhindret i at levere hele eller dele af de aftalte tjenester. Sådan manglende opfyldelse kan ikke tilskrives databehandlerens misligholdelse. Databehandleren opretholder sit krav på betaling for sådanne ydelser, uanset de ikke kan leveres til den dataansvarlige.

Hvor det er særligt aftalt, at databehandleren ikke må gøre brug af underdatabehandlere uden den dataansvarliges forudgående tilladelse, accepterer den dataansvarlige, at dette kan medføre, at databehandleren kan blive afskåret fra at opfylde Services. Hvis den dataansvarlige har afslået, at der foretages ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere, vil manglende levering af tjenester derfor ikke anses for en misligholdelse af parternes aftale vedrørende levering af Services, som kan tilskrives databehandleren i de tilfælde, hvor den manglende opfyldelse kan henføres til en underdatabehandlers forhold.

Bilag C - Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker i henhold til de indgåede Serviceaftaler mellem den dataansvarlige og databehandleren.

Databehandleren baserer sit ledelsessystem for informationssikkerhed på principperne i ISO 27001 sikkerheds-framework og har implementeret de relevante kontroller, standarden definerer. Derudover har databehandleren implementeret et ledelsessystem for sikker behandling af personoplysninger.

Kontrollerne styres i et ISMS-system for ISO 27001 og PIMS-system for GDPR. Herved dokumenteres kontroller løbende, og findings fra interne audits anvendes til løbende forbedringer.

Databehandleren revideres desuden en gang årligt, hvor der udarbejdes en ISAE 3402-erklæring for drift, hosting og support, samt en ISAE 3000-erklæring. Derudover opretholder og vedligeholder databehandleren løbende en ISO 27001:2022-certificering.

Seneste erklæringer og certifikat ligger altid tilgængelig her: Legal & Compliance in itm8.

Den dataansvarlige har instrueret databehandleren i at behandle data ud fra de Services, der er indgået aftale om og ud fra nedenstående instrukser.

C.1.1 Hosting og drift

Såfremt hosting og drift er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Opbevaring og backup samt de dertil knyttede behandlingsaktiviteter, som er nødvendige i forbindelse med leveringen af de aftalte tjenester, eller som er nødvendige for at opfylde en anmodning eller instruks fra den dataansvarlige. Behandlinger, som foretages af databehandleren omfatter:

- Backup og backupkontroller.
- Patch Management.
- Drift og vedligehold af systemer og infrastruktur.
- Virusscanning og opfølgning på virusalarmer.
- Installationer og konfigurationer.
- Håndtering af overvågningsalarmer.
- Dokumentation af assets, procedurer og kontroller.

C.1.2 Support

Såfremt support er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Databehandling foretages i overensstemmelse med ydelser forbundet med de supportydelser, parternes aftale vedrørende levering af Services indeholder eller specifikke sager, den dataansvarlige igangsætter.

C.1.3 Konsulentydelser

Såfremt Konsulentydelser er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Databehandling må udelukkende foretages på baggrund af konkret aftalte konsulentopgaver.

C.1.4 Databaseadministration

Såfremt databaseadministration er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Databehandling foretages i overensstemmelse med ydelser forbundet med de databaseadministrations ydelser, parternes aftale vedrørende levering af Services indeholder eller specifikke sager, den dataansvarlige igangsætter.

C.1.5 Konfiguration og udvikling

Såfremt konfiguration og udvikling er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Databehandling foretages i overensstemmelse med de opgaver der er aftalt med den dataansvarlige.

C.1.6 Drift og service af følgende applikationsservices

Såfremt drift og service af følgende applikationsservices er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker som led i levering de valgte applikationsservices til den dataansvarlige, som er nærmere specificeret i Servicesaftalen indgået mellem parterne, herunder:

- Backup.
- Support.
- Hosting.
- Drift og vedligehold.
- Konfigurering.
- Opdateringer.
- Dokumentation.

Og dertil knyttede behandlingsaktiviteter, som er nødvendige i forbindelse med leveringen af Services, eller som er nødvendige for at opfylde en anmodning eller instruks fra den dataansvarlige.

C.1.7 Sikkerhedsservices

Såfremt sikkerhedsservices er valgt som behandlingsaktivitet i skemaet i bilag A.1. gælder følgende:

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker som led i levering af de valgte sikkerhedsservices til den dataansvarlige, som er nærmere specificeret i Servicesaftalen indgået mellem parterne, herunder:

- Overvågning.
- Konfiguration.
- Rapportering.
- Vedligehold.
- Dokumentation.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle et generelt højt sikkerhedsniveau, som afspejler de typer af data, der behandles. Tekniske og organisatoriske foranstaltninger er implementeret ud fra ISO 27001 standarden, og relevante kontroller fra anneks-A er implementeret.

Derudover skal sikkerhedsniveauet afspejle de specifikke aftalte ydelser i parternes aftale vedrørende levering af Services. Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger der skal gennemføres for at etablere det aftalte sikkerhedsniveau.

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

På aftaleindgåelsestidspunktet indebærer forpligtelsen for databehandleren til at gennemføre sikkerhedsforanstaltninger, at databehandleren skal implementere og opretholde det sikkerhedsniveau, der er beskrevet i dokumentet "Organisatoriske og tekniske foranstaltninger". Dokumentet er tilgængeligt på Legal & compliance in itm8. Disse krav til sikkerhed udgør den dataansvarliges samlede krav til sikkerhedsforhold hos databehandleren ud fra den dataansvarliges egen risikovurdering.

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:

På den dataansvarliges specifikke anmodning bistår databehandleren 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 udøvelse af de registreredes rettigheder som fastlagt i databeskyttelsesforordningen.

Hvis en registreret fremsætter anmodning om udøvelse af sine rettigheder over for databehandleren, giver databehandleren uden ugrundet ophold meddelelse herom til den dataansvarlige.

Under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, bistår databehandleren efter specifik anmodning også den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i forhold til:

- Gennemførelse af passende tekniske og organisatoriske foranstaltninger.
- Sikkerhedsbrud.
- Underretning om brud på persondatasikkerheden til den registrerede.
- Gennemførelse af konsekvensanalyser.
- Forudgående høringer fra tilsynsmyndighederne.

C.4 Opbevaringsperiode/sletterutine

Den dataansvarlige disponerer selv over personoplysninger, som databehandleren behandler på vegne af den dataansvarlige. De personoplysninger, der er overladt til databehandlerens behandling, opbevares derfor, indtil den dataansvarlige selv sletter oplysningerne eller indtil ophør af Services vedrørende behandling af personoplysninger.

Ved sletning af personoplysninger i den dataansvarliges systemer, vil disse personoplysninger blive slettet i databehandlerens backupsystem ud fra den aftalte opbevaringsperiode (backuphistorik) for hvert enkelt system.

Databehandleren bistår på den dataansvarliges anmodning med sletning eller tilbagelevering af personoplysninger som nærmere instrueret af den dataansvarlige.

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 en eller flere af følgende adresser:

- Databehandlerens adresser.
- Datacentre databehandleren benytter.
- Underdatabehandlere, samt deres underdatabehandleres adresser.

Derudover kan der udføres remote arbejde i overensstemmelse med databehandlerens retningslinjer for remote arbejde.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Den dataansvarlige har bemyndiget og dermed instrueret databehandleren i at overføre personoplysninger til et tredjeland som nærmere specificeret nedenfor. Den dataansvarlige kan herudover ved en efterfølgende skriftlig meddelelse eller aftale angive en instruks eller konkret godkendelse vedrørende overførsel af personoplysninger til et tredjeland.

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

C.6.1 Generel godkendelse vedrørende overførsel af personoplysninger til sikre tredjelande

Den dataansvarlige giver ved Bestemmelserne sin generelle og forudgående godkendelse (instruks) til, at databehandleren kan foretage overførsel af personoplysninger til tredjelande, hvis Kommissionen har fastslået, at tredjelandet/det relevante område/den relevante sektor har et tilstrækkeligt beskyttelsesniveau.

For overførsler til organisationer i USA, som er certificerede under EU-U.S. Data Privacy Framework ("DPF"), giver den dataansvarlige også ved Bestemmelserne sin generelle og forudgående godkendelse (instruks) til, at databehandleren kan foretage overførsler af personoplysninger til disse organisationer. Databehandleren er til enhver tid forpligtet til at sikre, at anvendte underdatabehandlere har den påkrævede certificering.

C.6.2 Godkendelse af overførsel til specifikke modtagere af personoplysninger i tredjelande

Den dataansvarlige instruerer databehandleren i at anvende de underdatabehandlere, der til enhver tid fremgår af nedenstående liste, herunder underdatabehandlere der overfører personoplysninger til tredjelande: https://legal.itm8.com/Default.aspx?ID=12265&Purge=True

Ved indgåelsen af Bestemmelserne har den dataansvarlige godkendt anvendelsen af de underdatabehandlere, der fremgår af ovenstående liste, samt instrueret databehandleren i at overføre personoplysninger til tredjelande i det omfang, det er nødvendigt for leveringen af Services.

Såfremt EU-Kommissionens standardkontrakter ("SCC") for overførsel af personoplysninger til et tredjeland anvendes som overførselsgrundlag, er databehandleren og/eller evt. underdatabehandleren berettiget til at indgå disse SCC'er med den relevante underdatabehandler.

I tilfælde af at EU-Kommissionen udarbejder nye SCC'er efter aftaleindgåelsen, er databehandleren bemyndiget til at udskifte, opdatere og anvende de til enhver tid gældende SCC'er.

Indholdet af denne instruks og/eller Bestemmelserne anses ikke for at ændre indholdet af SCC.

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

Den dataansvarlige har efter databeskyttelsesforordningens art. 24 og 28 ret og pligt til at gennemføre tilsyn med databehandlerens behandling af personoplysninger på den dataansvarlige vegne. Den dataansvarliges gennemførelse af tilsyn med databehandleren kan ske ved, at den dataansvarlige udfører en af følgende handlinger:

- egenkontrol på baggrund af dokumenter, som databehandleren gør tilgængelig for den dataansvarlige.
- skriftligt tilsyn eller
- fysiske inspektioner.

C.7.1 Egenkontrol

Den dataansvarlige har på Legal & Compliance in itm8 adgang til en række dokumenter til brug for gennemførelse af egenkontrol, herunder:

- Nyeste version af databehandlerens ISAE 3402-erklæring (publiceres hvert år).
- Nyeste version af databehandlerens ISAE 3000-erklæring (publiceres hvert år).
- Nyeste version af ISO 27001-certifikat.
- Beskrivelse af organisatoriske og tekniske foranstaltninger hos databehandleren.
- Informationssikkerhedspolitik.

C.7.2 Skriftligt tilsyn og fysisk inspektion

Den dataansvarlige kan vælge at gennemføre et tilsyn enten som skriftligt tilsyn eller ved fysisk inspektion. Tilsynet kan udføres af den dataansvarlige selv og/eller i samarbejde med tredjepart. Et tilsyn skal tage udgangspunkt i de sikkerhedsforanstaltninger, der er aftalt mellem parterne.

Ved anmodning om gennemførelse af skriftligt tilsyn eller fysisk inspektion anvendes nedenstående fremgangsmåde.

Procedure og rapportering for skriftligt tilsyn eller fysisk inspektion:

- Den dataansvarlige sender deres tilsynsskema til databehandleren via e-mail til gdpr@itm8.com ønske om gennemførelse af tilsyn og/eller inspektion.
- Databehandleren bekræfter modtagelse og oplyser endelig dato for gennemførelse af tilsynet og/eller inspektion.
- Gennemførelsen af tilsynet og/eller inspektion finder sted.

- Den dataansvarlige fremsender eventuelle observationer fra tilsynet til gdpr@itm8.com.
- Databehandleren gennemgår og kommenterer på den dataansvarliges eventuelle observationer (kan gentages flere gange).
- Den dataansvarlige udfører sin endelige konklusion på tilsynet og fremsender rapporten til databehandleren.
- Tilsynet afsluttes.

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

Databehandleren udfører, på baggrund af databehandlerens risikovurdering og under hensyntagen til de konkrete behandlingsaktiviteter, revisioner, herunder inspektioner, med underdatabehandleres behandling af personoplysninger enten i form af egenkontrol af revisionserklæringer og tilsvarende (hvor muligt), skriftligt tilsyn eller fysisk inspektion, eller en kombination heraf.

Den dataansvarlige kan på den dataansvarliges anmodning få yderligere oplysninger om, hvilke kontrolforanstaltninger der er iværksat og gennemført over for de enkelte underdatabehandlere.

Bilag D – Parternes regulering af andre forhold

D.1 Generelt

I relation til databehandlerens behandling af personoplysninger på vegne af den dataansvarlige har parterne aftalt nedenstående supplerende vilkår.

Bestemmelserne i denne aftale har forrang i forhold til eventuel tilsvarende regulering i Serviceaftaler mellem parterne vedrørende den del af databehandlerens aktiviteter og ansvar der knytter sig til databehandlingen, mens udførelsen af alle andre aktiviteter vedrørende leveringen af aftalte Services er underlagt de øvrige dele af Serviceaftalen.

Serviceaftalens øvrige vilkår, herunder ansvarsbegrænsninger m.v., er også gældende for databehandlerens opfyldelse af disse Bestemmelser.

I tilfælde af uoverensstemmelse mellem Bestemmelserne og de i dette bilag D fastsatte vilkår skal bilag D have forrang, og såfremt Serviceaftalen i øvrigt indeholder vilkår om databehandlerens behandlingsaktiviteter, vil bilag D ligeledes have forrang.

D.2 Konsekvenser af den dataansvarliges ulovlige instruks

Den dataansvarlige er bekendt med, at databehandleren er afhængig af den dataansvarliges anvisninger om, i hvilket omfang databehandleren er berettiget til at anvende og behandle personoplysningerne på den dataansvarliges vegne. Databehandleren hæfter derfor ikke for krav, som udspringer af databehandlerens handlinger eller undladelser, i det omfang disse handlinger eller undladelser er en databehandlingsaktivitet udøvet i overensstemmelse med den dataansvarliges instrukser.

D.3 Implementering af andre sikkerhedsforanstaltninger

Databehandleren er berettiget til at implementere og opretholde alternative sikkerhedsforanstaltninger i forhold til det i aftalen vedrørende levering af Services og bilag C.2 anførte, dog under forudsætning af at sådanne alternative sikkerhedsforanstaltninger samlet set sikrer et sikkerhedsniveau på niveau med de foreskrevne sikkerhedsforanstaltninger.

D.4 Anvendelse af Tredjepartsydelser

Uanset Bestemmelsernes punkt 7 er det aftalt, at dersom databehandleren anvender underdatabehandlere der i en Serviceaftale er identificeret som leverandør af Standard Tredjepartsydelser, vil Tredjepartsleverandørers eventuelle behandlingsaktiviteter (som underdatabehandler) i forbindelse med leveringen af disse Standard Tredjepartsydelser være underlagt Tredjepartpartsleverandørens egne vilkår for behandlingsaktiviteterne som underdatabehandler.

Databehandleren har gjort vilkårene tilgængelige på https://legal.itm8.com, og det er den dataansvarliges eget ansvar at gøre sig bekendt med disse og i øvrigt sikre sig, at disse vilkår på tilfredsstillende vis opfylder krav til Tredjepartsleverandørens behandlingsaktiviteter.

Den dataansvarlige er gjort bekendt med, at disse vilkår løbende kan ændres af den enkelte Tredjepartsleverandør, og den dataansvarlige skal således kontinuerligt sikre sig, at disse opfylder kravene til behandlingsaktiviteterne.

Den dataansvarlige kan til hver en tid kontakte databehandleren med henblik på at få vilkårene udleveret.

Ved sin accept af Bestemmelserne giver den dataansvarlige samtidig sin accept af, og instruks til, at behandlingsaktiviteter sker på Tredjepartsleverandørens vilkår.

D.5 Sletning og returnering af oplysninger

Det er mellem parterne aftalt, at den dataansvarlige instruerer om databehandlerens sletning og returnering af personoplysninger i forbindelse med Bestemmelsernes ophør.

Den dataansvarlige skal, senest 30 dage efter at behandlingen af personoplysninger er ophørt, meddele databehandleren, hvorvidt alle personoplysninger skal slettes eller tilbageleveres til den dataansvarlige. I det tilfælde hvor personoplysninger skal tilbageleveres til den dataansvarlige, skal databehandleren ligeledes slette eventuelle kopier. Databehandleren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever meddelelsen fra den dataansvarlige.

Sletningspligten omfatter ikke (i) kopier af elektronisk udvekslede personoplysninger opbevaret som led i automatiserede backup funktioner, forudsat at adgangen hertil er begrænset til IT- eller compliancepersonale og forudsat at sådanne oplysninger fortsat behandles i overensstemmelse med Bestemmelserne, og (ii) personoplysninger som skal opbevares af databehandleren ifølge ufravigelig lovgivning.

Såfremt databehandleren ikke har modtaget meddelelse fra den dataansvarlige, inden 30 dage efter behandlingen af personoplysninger er ophørt, fremsender databehandleren en rykker til den dataansvarlige. Hvis den dataansvarlige herefter ikke meddeler databehandleren, hvorvidt alle personoplysninger skal slettes eller tilbageleveres til den dataansvarlige, er databehandleren uden yderligere varsel berettiget til at slette personoplysninger.

Databehandleren er berettiget til vederlag for dennes behandlingsaktiviteter frem til det tidspunkt, hvor den dataansvarlige meddeler databehandleren, hvorvidt alle personoplysninger skal slettes eller tilbageleveres til den dataansvarlige.

D.6 Vederlag

D.6.1 Bistand - generelt

Medmindre databehandleren som led i aftalte Services og indenfor det faste vederlag for sådanne Services har påtaget sig at opfylde Bestemmelserne, vil databehandleren være berettiget til vederlag for bistand efter de i Bestemmelsernes, herunder punkt 9, aftalte bistandsydelser.

Vederlaget opgøres på baggrund af den forbrugte arbejdstid og de aftalte timesatser i Serviceaftale vedrørende levering af Services, og hvor der ikke er aftalt timesatser heri, da efter databehandlerens gældende timesatser.

Eventuelt afholdte eksterne omkostninger, herunder også omkostninger der skal afholdes af databehandleren for underdatabehandleres bistand, faktureres den dataansvarlige.

D.6.2 Implementering af øvrige sikkerhedsforanstaltninger

Såfremt den dataansvarliges instrukser m.v., samt databehandlerens løbende vurderinger i øvrigt, medfører skærpede krav til de i en Serviceaftale indeholdte krav til sikkerhedsforanstaltninger vedrørende leveringen af Services eller til bilag C, vil databehandleren loyalt søge at imødekomme sådanne krav såfremt dette er teknisk muligt og foreneligt med opfyldelsen af øvrige krav til de berørte Services.

Databehandleren er berettiget til vederlag og omkostningsdækning efter samme principper som ovenfor.

D.6.3 Tilsyn og revision

Databehandleren er berettiget til vederlag for den dataansvarliges udøvelse af tilsyn og revision. Vederlaget opgøres på baggrund af den forbrugte arbejdstid og de aftalte timesatser i Serviceaftale vedrørende levering af Services, og hvor der ikke er aftalt timesatser heri, da efter databehandlerens gældende timesatser.

Eventuelt afholdte eksterne omkostninger, herunder også omkostninger der skal afholdes af databehandleren for underdatabehandleres bistand, faktureres den dataansvarlige.

D.7 Ansvar og misligholdelse

En eventuel misligholdelse af Bestemmelserne reguleres og behandles i overensstemmelse med parternes Serviceaftale vedrørende levering af Services, med følgende tillæg;

a) I tilfælde hvor databehandleren har udredt beløb til registrerede i overensstemmelse med databeskyttelsesforordningens artikel 82 eller erstatningsansvarsloven § 26, har databehandleren fuld regres mod den dataansvarlige for det udredte beløb, som beløbsmæssigt overstiger den aftalte ansvarsbegrænsning i parternes Serviceaftale vedrørende levering af Services. Parterne har hermed aftalemæssigt fraveget databeskyttelsesforordningens artikel 82, stk. 5 og erstatningsansvarsloven § 26.

b) Uanset databeskyttelsesforordningen art 82, stk. 5 kan databehandleren, dersom denne har udredt erstatningsbeløb til en skadelidt, der ikke svarer til fuld erstatning, gøre regres efter princippet i art. 82, stk. 5.

c) I forhold til anden godtgørelse for ikke-økonomiske tab til de registrerede skal princippet i art. 82 ligeledes finde anvendelse, for så vidt angår den interne endelige ansvarsfordeling mellem databehandleren og den dataansvarlige.

d) Parterne kan ikke gøre regres eller erstatningskrav gældende overfor den anden part for bøder eller anden straf, der er pålagt i medfør af databeskyttelsesloven § 41 samt for bødeforelæg accepteret efter databeskyttelsesloven § 42.

e) Databehandlerens samlede erstatningsansvar ved misligholdelse af Bestemmelserne er omfattet af den beløbsmæssige begrænsning (og indregnes ved erstatningsmaksimeringen) der eventuelt følger af parternes Serviceaftale. Ansvaret (inklusiv sådan erstatning eller anden økonomisk kompensation der måtte være indrømmet den dataansvarlige under Serviceaftalen) begrænses til et beløb lavere end 150% af det beløb databehandleren har modtaget i de foregående 12 måneder forud for den skadegørende handling. Såfremt en 12 måneders periode ikke er gået, beregnes ansvarsbegrænsningen som gennemsnittet af modtagne beløb i de måneder, som er gået, ganget med 12.

f) Databehandlerens erstatningsansvar ved misligholdelse af Bestemmelserne omfatter ikke indirekte tab, herunder driftstab, følgeskader eller andet indirekte tab.

g) Databehandleren er ikke ansvarlig for misligholdelse af Bestemmelserne forårsaget af computervirus, cyberkriminalitet eller andre former for tredjemands uberettigede indgreb i den

dataansvarlige eller databehandlerens IT-systemer, medmindre tabet er direkte relateret til manglende opfyldelse af aftalte krav til sikkerhed i parternes Serviceaftale.

D.8 – Særskilte nationale krav til databeskyttelse

Såfremt den dataansvarlige er beliggende uden for Danmark, finder særskilte krav anvendelse, som er i overensstemmelse med nationale databeskyttelsesregler i den dataansvarliges hjemland. De nationale særregler findes her: https://legal.itm8.com/Default.aspx?ID=12295&Purge=True