itm8®

Itm8 | Improsec A/S

Bilag A-C under itm8 Group's Databehandleraftale

Indholdsfortegnelse

itm8 Group's Databehandleraftales bilag A-C	2
Baggrund	2
Bilag A – Oplysninger om behandlingen	3
Bilag B – Underdatabehandlere	6
Bilag C - Instruks vedrørende behandling af personoplysninger	8

itm8 Group's Databehandleraftales bilag A-C

Baggrund

I henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) og med henblik på understøttelse af databehandlerens behandling af personoplysninger har Kunden (herefter "den dataansvarlige") og Leverandøren (herefter "databehandleren") tiltrådt itm8 Group's Databehandleraftale (herefter "Bestemmelserne"), som er tilknyttet den gældende Samarbejdsaftale (herefter "Samarbejdsaftalen") mellem parterne.

Parterne har under Samarbejdsaftalen indgået Work Order af den [dato] for levering af [ydelse/service], som er tilknyttet Samarbejdsaftalen.

Databehandleren foretager som led i opfyldelsen af denne Work Order behandlinger af personoplysninger, og som tillæg til den gældende Work Order og den tiltrådte itm8 Group's Databehandleraftale, har parterne på den baggrund tiltrådt dette **Bilag A-C**.

Bilag A-C udgør således et bilag til den gældende Work Order og indeholder de specifikke krav i forhold til f.eks. den dataansvarliges instrukser, behandlingens genstand, behandlingens karakter, brugen af underdatabehandlere, sikkerhedsforanstaltning mv.

Bilag A-C skal anses som en integreret del af Samarbejdsaftalen for levering af de Services, som er specificeret i den pågældende Work Order, og Bilag A-C træder som konsekvens heraf i kraft samtidig med indgåelsen af den gældende Work Order, og er gældende indtil denne ophører, medmindre parterne tiltræder et nyt Bilag A-C, som erstatter dette Bilag A-C.

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)	FORMÅLET MED BEHANDLINGEN
☐	Konsulentydelser

A.1.1 Konsulentydelser

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

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

A.2.1 Konsulentydelser

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

Almindelige personoplysninger (jf. Databeskyttelsesforordningens artikel 6):

☒ Navn

☒Adresse

☒ E-mail

☒ Telefonnummer

☒ Finansielle oplysninger

☐ Andre personoplysninger som nærmere specificeret:

... Specificer andre kategorier

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

☐Andre kategorier som nærmere specificeret.

... Specificer andre kategorier

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

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

NAVN/ADRESSE	CVR	LOKATION FOR BEHANDLING	BESKRIVELSE AF BEHANDLING
Microsoft Ireland Operations, Ltd. South County Business Park Leopardstown	SE-no.: IE8256796U	Data is stored within the EU, but support can be provided from around the world	Microsoft O365 and Azure

Listen over anvendte underdatabehandlere ved aftaleindgåelse er indsat i ovenstående skema, og bliver reguleret ved tilkøb eller ændringer i services.

Efter Bestemmelsernes ikrafttræden må databehandleren gøre brug af andre underdatabehandlere. Den dataansvarlige vil blive informeret om ændringer i anvendte underdatabehandlere ved tilkøb af nye services eller databehandlerens ændringer af services. Derudover kan et bilag over aktuelt anvendte underdatabehandlere leveres ved forespørgsel.

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.

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 Services. 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.

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 Konsulentydelser

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

Databehandling må udelukkende foretages på baggrund af konkret aftalte konsulentopgaver.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle et generelt højt sikkerhedsniveau, som afspejler de typer af data, der behandles. Tekniske og organisatoriske foranstaltninger er implementeret i henhold til ISO 27001-standarden, og kontroller fra ISO 27002 er implementeret og efterleves.

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 https://legal.itm8.com. 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 følgende:

Behandling af personoplysninger sker på en eller flere af følgende adresser:

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

Herudover kan der udføres remote arbejde i overensstemmelse med databehandlerens politik 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 til at anvende nedenstående underdatabehandler(e), hvor der sker overførsel af personoplysninger til tredjelande:

NAVN	CVR	BESKRIVELSE AF BEHANDLING	OVERFØRSEL TIL TREDJELAND

Den dataansvarlige har ved indgåelsen af Bestemmelserne givet godkendelse til brugen af ovenstående underdatabehandler(e) samt instruks om overførelse af personoplysninger til tredjelande ved levering 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 https://legal.itm8.com adgang til en række dokumenter til brug for gennemførelse af egenkontrol, herunder:

- 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@improsec.com med 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@improsec.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.