



FRONTLINERS

DATABEHANDLERAFTALE



Standardkontraksbestemmelser

Side 2 af 21

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

mellem

Navn
CVR-nummer
Adresse
Postnummer og By
Land

herefter "den dataansvarlige"

og

Frontliners ApS
CVR 38865366
Flæsketorvet 68
1711 København V
Danmark

herefter "databehandleren"

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

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



1. Indhold	
2. Præambel	4
3. Den dataansvarliges rettigheder og forpligtelser	4
4. Databehandleren handler efter instruks.....	5
5. Fortrolighed.....	5
6. Behandlingssikkerhed	5
7. Anvendelse af underdatabehandlere	6
8. Overførsel til tredjelande eller internationale organisationer	7
9. Bistand til den dataansvarlige	8
10. Underretning om brud på persondatasikkerheden	9
11. Sletning og returnering af oplysninger	10
12. Revision, herunder inspektion	10
13. Parternes aftale om andre forhold	10
14. Ikrafttræden og ophør	10
15. Kontaktpersoner hos den dataansvarlige og databehandleren	11
Bilag A Oplysninger om behandlingen	12
Bilag B Underdatabehandlere	13
Bilag C Instruks vedrørende behandling af personoplysninger	15
Bilag D Parternes regulering af andre forhold.....	21



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 Frontliners medarbejderplatform 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 er 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 medlemsstaternes¹ nationale ret og disse Bestemmelser.

¹ Henvisninger til "medlemsstat" i disse bestemmelser 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 30 dages 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 indføre 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. indsigtretten
 - 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 insigelse
 - 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 unødigt 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 unødigt 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 unødigt 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 72 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 dataansvarlige, 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. Procedurene 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 u hensigtsmæssigheder 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

Side 11 af 21

Navn

Stilling

Telefonnummer

E-mail

Underskrift – er afgivet ved accept af betingelser ved oprettelse af virksomheden i databehandlerens platform.

På vegne af databehandleren

Navn Danny Fabricius Fogel

Stilling CEO

Telefonnummer +45 31 20 48 00

E-mail danny@frontliners.ai

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.

Hos den dataansvarlige

Acceptgiver ved oprettelse på Frontliners platformen.

Hos databehandleren

Navn Danny Fabricius Fogel

Stilling CEO

Telefonnummer +45 31 20 48 00

E-mail danny@frontliners.ai



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

Databehandleren stiller på abonnementsbasis Frontliners medarbejderplatform cloud-baserede tjenester ("Tjenester") til rådighed for den dataansvarlige og dennes medarbejdere. Tjenesterne kan dels tilgås via databehandlerens hjemmeside app.frontliners.ai, og dels via databehandlerens app.

Den dataansvarliges brug af databehandlerens cloud-baserede Tjenester sker ved den dataansvarliges selvbetjening via databehandlerens hjemmeside, og/eller via databehandlerens app. Den dataansvarliges medarbejdere kan ligeledes tilgå deres egne oplysninger, så som vagtplaner, personoplysninger, ferieoversigter, og de dokumenter, som medarbejderen eller kunden har indlæst, eksempelvis ansættelseskontrakt. Både den dataansvarliges og dennes medarbejders brug kræver et bruger ID og en unik adgangskode.

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

Opbevaring og foretagelse af vagtplan administration, HR-administration, medarbejderens engagement og kommunikation med virksomheden, samt beregning af løn, tidsregistrering, registrering af ferie, fraværsregistrering o.lign.

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

De personoplysninger, som behandles af databehandleren i forbindelse med den dataansvarliges brug af databehandlerens Tjenester er forskellige alt efter hvilken kategori den registrerede tilhører, jf. følgende oversigt:

KATEGORIER AF DATASUBJEKTER	PERSONOPLYSNINGER
Kunder	<ul style="list-style-type: none">• Kontaktpersoner hos den dataansvarlige, herunder disses kontaktoplysninger, så som telefon, email, titel, afdeling, adresse• Kreditkortoplysninger til brug for betalingen.
Den dataansvarliges nuværende og tidligere medarbejdere	<ul style="list-style-type: none">• Navn• Adresse• CPR-nummer• Kontaktoplysninger, herunder telefon, email, titel, afdeling, adresse• Navn og kontaktoplysninger for medarbejdernes pårørende• Løn• Fravær (f.eks. grundet sygdom, barsel, militærtjeneste, borgerligt• ombud, periodiske ansættelser, o.s.v.)• Opgørelse af feriedage• Time-/tidsregistreringer



	<ul style="list-style-type: none"> • Registrering af enheder og adgange, som er tildelt medarbejderen • Oversigt over medarbejderens handlinger i systemet. • Uploadede dokumenter (f.eks. ansættelseskontrakt, MUS-samtaler, straffeattest, o.s.v.)
Den dataansvarliges nuværende og tidligere ansøgere	<ul style="list-style-type: none"> • Navn • Telefonnummer • E-mailadresse

A.4. Behandlingen omfatter følgende kategorier af registrerede

Se oversigten i afsnit A.3.

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige fortsætter så længe den dataansvarlige gør brug af de Tjenester, som den dataansvarlige abonnerer på hos databehandleren.

Ved abonnementsaftalens ophør får den dataansvarlige valget imellem, om data skal slettes efter 7 dage, eller om den dataansvarlige ønsker opbevaring af og adgang til data i 6 måneder. Hvis den dataansvarlige inden udløbet af en valgt 7 dages eller 6 måneders periode fortsat ønsker opbevaring af data hos databehandleren, skal den dataansvarlige genaktivere abonnementet.

Hvis en medarbejders tilknytning til den dataansvarlige ophører, har medarbejderen fortsat adgang til egne oplysninger indtil den dataansvarlige vælger at slette oplysningerne. Ved den dataansvarliges beslutning om sletning af oplysningerne modtager medarbejderen tilbud om muligheden for fortsat opbevaring af medarbejderens egne oplysninger i henhold til en separate dataopbevaringsaftale

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes i krafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Stripe	IE 3206488LH	Stripe Payments Europe, Limited The One Building 1 Grand Canal Street Lower Dublin 2 Co. Dublin Ireland	Fakturering og opkrævning af Frontliners kunder



NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Microsoft Azure	IE8256796U	Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park Leopardstown Dublin 18, D18 P521 Ire-land	Dataopbevaring og databehandling
Atomchat	EU372017215	Judd House 18-29 Mora Street London, EC1V 8BT United Kingdom	Opbevaring af navne til brug i Frontliners Messenger. Notifikationer.
HubSpot Ireland Ltd	IE9849471F	Ground Floor, Two Dockland Central, Guild Street, Dublin 1, Co. Dublin, Ire-land	Kunde support Ticket system
Userflow	EIN35-2628653	548 Market St PMB 69598, San Francisco, CA 94104-5401, USA	Onboarding
Sendgrid		375 Beale Street, 3rd Floor, San Francisco, CA 94105	Transaktionelle e-mails, herunder nulstilling af adgangskoder.
Frontliners ApS		Flæsketorvet 68, 1711 København V	Drift, support og udvikling af Applikationen

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

Se Bestemmelse 7.3.



C.1. Behandlingens genstand/instruks

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

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

Ved den dataansvarliges brug af databehandlerens tjenester – hvad enten sådan brug foretages af den dataansvarlige eller en af denne udpeget medarbejder – behandler databehandleren persondata vedrørende den dataansvarliges medarbejdere i forbindelse med den dataansvarliges administration for egne medarbejdere, herunder løn, ferie- og fravær, tidsregistrering, administration af enheder og adgange tildelt den enkelte medarbejder, kursusadministration og lagring af dokumenter, eksempelvis ansættelseskontrakt.

Den dataansvarlig og/eller dennes medarbejdere indlæser selv de oplysninger, som er nødvendige for brug af Tjenesterne. Herudover instruerer den dataansvarlige Frontliners i løbende og automatisk at indhente oplysninger fra relevante myndigheder, for at sikre, at de anvendte oplysninger om medarbejdernes forhold er opdaterede, når Tjenesterne bruges.

Tjenesterne er udviklet med åbent API, som gør det muligt for andre at udvikle og tilbyde apps, der kan kommunikere med Applikationen, herunder udveksle oplysninger på tværs af programmerne ("Tredjeparts-app(s)"). I det omfang den dataansvarlige vælger at installere og gøre brug af Tredjeparts-apps, der kan kommunikere med Applikationen, anses det for at udgøre en instruktion til Frontliners om, at der kan ske overførsel af de i Applikationen indtastede/indlæste og de af Applikationen genererede oplysninger til sådanne Tredjeparters apps.

Den dataansvarlige accepterer desuden, at dennes Medarbejdere har mulighed for at installere og gøre brug af Tredjeparts-apps, der kan kommunikere og udveksle den enkelte Medarbejders oplysninger med Applikationen, og at sådan databehandling er omfattet af instruksens ifølge denne aftale.

Den dataansvarligere giver tilsvarende instruks om, at også den dataansvarliges medarbejdere kan vælge at installere og gøre brug af Tredjeparts-apps, der kan kommunikere med Applikationen, og instruere Frontliners i, at der i så fald kan ske overførsel af de i Applikationen indtastede/indlæste og de af Applikationen genererede oplysninger, som Medarbejderen har adgang til, til sådanne Tredjeparters apps.

Frontliners er berettiget til at behandle de i Bilag A.3 angivne personoplysninger til egne formål som selvstændig dataansvarlig ved ophør af abonnementsaftalen med den dataansvarlige.

Frontliners er desuden berettiget til at opbevare de i Bilag A.3 angivne personoplysninger med det formål at kunne udsende nyhedsbreve og underrette om nye forhold hos Frontliners, såfremt den pågældende person har samtykket hertil, anonymisere oplysningerne til statistiske formål således at hverken person eller virksomhed kan identificeres, behandle oplysningerne som påkrævet i henhold til lovgivningen, herunder i forbindelse med en retlig afgørelse, myndighedskrav, den dataansvarliges konkurs, dødsfald eller lignende.

Der henvises i øvrigt til de aftalte vilkår i Frontliners abonnementsbetingelser.



C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Behandlingen af data omfatter personoplysninger omfattet af databeskyttelsesforordningen artikel 9 om særlige kategorier af personoplysninger, hvorfor der er etableret et højt sikkerhedsniveau.

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.

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

Service og database lokation:

Frontliners databaser er lokaliseret i North Europe – Dublin – Ireland

Der kan læses mere om Azure lokationer her: <https://azure.microsoft.com/da-dk/global-infrastructure/regions/>

Data kryptering

Data er krypteret både under transport og "at rest".

Database tilgængelighed

Data opbevares i Azure. IP skal manuelt tilføjes til Azure af administratoren for at få adgang. Adgangen er begrænset til meget få brugere.

Passwords

Passwords er SHA256 krypteret med unik salt.

Backup

Frontliners bruger Cloudflare til at hoste sin applikation og Azure til at hoste sit API. Backup politikken er sat til at bevare alle tidligere versioner.

Frontliners bruger Azure til at hoste sin database. Backup politikken er sat til at tage fuld backup hver uge.

Yderligere er funktionen "Point-in-time" backup sat op således at databasen kan genskabes til et hvilket som helst tidspunkt 35 dage tilbage i tiden.

Der kan læses mere om Azure continuity her: <https://azure.microsoft.com/en-us/updates/point-in-timerestore-retention-for-standard-edition-extended-to-35-days/>

Tredjepart og leverandør risikovurdering

Frontliners gennemfører årlige reviews af sine leverandører og tredjepartere. Det sker konkret ved gennemgang af databehandleraftaler for de enkelte leverandører, en risiko vurdering og en omfangsvurdering.

Risiko og omfang er inddelt i tre kategorier

Risiko

Lav risiko

- 5 personer eller færre har adgang til ressourcen
- Adgang til ressourcen sker med komplekse adgangskoder



- Adgang til ressourcen sker med to faktor og/eller certifikat baseret adgang

Mellem risiko

- Flere end 5 personer har adgang til ressourcen
- Data kan stamme fra flere kilder
- Frontliners har ikke fuld kontrol over data
- Adgang til ressourcen sker med komplekse adgangskoder og/eller to faktor

Høj risiko

- Flere end 5 personer har adgang til ressourcen
- Adgang til ressourcen sker med simple adgangskoder

Omfang

Lavt omfang

- Omfang af et datalæk er lavt
- Eksempel: Ikke identificerbar information, ikke personfølsom information.

Mellem omfang

- Omfang af et datalæk er mellem
- Eksempel: Identificerbar information så som navne, adresser og mails.

Højt omfang

- Omfang af et datalæk er højt
- Eksempel: Brugernavne og adgangskoder, helbredsinformationer, CPR-numre, religiøse og fagforenings tilhørsforhold.

Brugers adgang til data via browser

Adgang sker via internettet via en webbrowser der understøtter https.

Frontliners har implementeret mulighed for ejere af en Frontliners konto til at opretholde egen adgangskode.

Hjemmearbejdspladser

Medarbejdere har mulighed for at arbejde hjemmefra.

Alle computere er krypterede og adgangskodebeskyttet.

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 sådanne tekniske og organisatoriske foranstaltninger, som kan bidrage til den dataansvarliges mulighed for at besvare anmodninger om udøvelsen af de registreredes rettigheder.

C.4 Opbevaringsperiode/sletterutine

Data opbevares så længe den dataansvarlige finder, at det opfylder det formål som den dataansvarlige har. Frontliners stiller funktioner til rådighed for den dataansvarlige, således at den dataansvarlige kan leve op til de formål.

Såfremt den dataansvarlige op siger sin aftale med Frontliners, har Frontliners bygget funktionalitet der muliggør eksport og sletning af data på to måder – den valgte måde afhænger af den dataansvarliges nærmere instruks:

- Eksporter al data og slet data inden for 7 dage
- Eksporter al data og slet data inden for 6 måneder

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:



C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Den dataansvarlige er bekendt med – og er forpligtet til at gøre sine medarbejdere bekendt med – at databehandlerens Tjenester stilles til rådighed via en cloud-baseret løsning, hvor databehandleren blandt andet gør brug af software og IT-systemer, herunder servere, der stilles til rådighed af tredjeparter.

I det omfang databehandlerens Tjenester gør brug af eller er baseret på ydelser, der leveres af underdatabehandlere i tredjelande, meddeler den dataansvarlige hermed instruks og bemyndigelse til databehandleren om at overføre persondata til databehandlerens underdatabehandlere i sådanne tredjelande til brug for databehandlerens levering af de Tjenester som den dataansvarlige abonnerer på hos databehandleren.

Brugen af underdatabehandlere i tredjelande skal være underlagt tilsvarende bestemmelser som de Bestemmelser, der er aftalt mellem den dataansvarlige og databehandleren, ligesom databehandleren er forpligtet til at sikre, at overførslen og databehandlingen sker i henhold til gældende EU standardklausuler for overførsel af personoplysninger (EU standardbestemmelser).

Databehandleren skal i sin aftale med underdatabehandlere indføre 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, jf. Bestemmelse 7.6.

Overførslen til tredjelande sker i henhold til EU-Kommissionens standardbestemmelser om databeskyttelse. Den dataansvarlige giver hermed fuldmagt til databehandleren til at indgå aftaler med underdatabehandlerne i de pågældende tredjeland på den dataansvarliges vegne baseret på EU-Kommissionens Standardbestemmelser for overførsel mellem en dataansvarlig i EU til en databehandler uden for EU.

Se tillægsaftale om EU Standardkontraktbestemmelser.

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

Databehandleren skal i perioden februar til juni hvert år for egen regning indhente en revisionserklæring fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisionserklæringer kan anvendes i overensstemmelse med disse Bestemmelser:

- ISAE 3402

Revisionserklæringen gøres uden unødigt forsinkelse offentligt tilgængelig på databehandlerens hjemmeside, www.frontliners.ai til den dataansvarlige til orientering.



Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde for egen regning og risiko anmode om en ny revisionserklæring under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæringen, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Databehandler stiller muligheden til rådighed for den dataansvarlige eller en repræsentant for den dataansvarlige for at foretage en årlig inspektion, herunder fysisk inspektion, af lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådant en inspektion gennemføres, årligt når databehandler indkalder til mulighed for inspektion typisk på en dato i september eller oktober.

Den dataansvarliges og databehandlerens eventuelle udgifter i forbindelse med en inspektion afholdes af den dataansvarlige selv, jf. Bilag D.

Bestemmelse 12.1. Databehandleren er forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion.

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

Databehandleren eller en repræsentant for databehandleren kan foretage årligt en fysisk inspektion af lokaliteterne, hvorfra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen, med henblik på at fastslå underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Ud over det planlagte tilsyn, kan databehandleren gennemføre en inspektion med underdatabehandleren, når databehandleren finder det nødvendigt.

Dokumentation for sådanne inspektioner fremsendes uden unødigt forsinkelse til den dataansvarlige til orientering.

Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde for egen regning og risiko anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af tilsynet, er den dataansvarlige berettiget til for egen regning og risiko at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarlige kan for egen regning og risiko vælge at initiere og deltage på en fysisk inspektion hos underdatabehandleren. Dette kan blive aktuelt, hvis den dataansvarlige vurderer, at databehandlerens inspektion hos underdatabehandleren ikke har givet den dataansvarlige tilstrækkelig sikkerhed for, at behandlingen hos underdatabehandleren sker i overensstemmelse med databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.



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

Databehandlerens og underdatabehandlerens udgifter i forbindelse med en fysisk inspektion af underdatabehandlerens lokaliteter er den dataansvarlige uvedkommende, med mindre inspektionen er initieret af den dataansvarlige jf. Bilag D, Bestemmelse 12.1.



Bilag D Parternes regulering af andre forhold

Side 21 af 21

Som supplement til Bestemmelserne har Parterne aftalt følgende:

Vedr. Bestemmelse 4.2:

Uanset Bestemmelse 4.2, er databehandleren ikke forpligtet til aktivt at efterprøve eller undersøge lovligheden af den dataansvarliges instrukser.

I det omfang den dataansvarlige giver instrukser til databehandleren, som efterfølgende viser sig at være ulovlige, er den dataansvarlige forpligtet til at friholde databehandleren for ethvert tab som følge heraf, herunder at friholde databehandleren for ethvert krav mod databehandleren, der følger heraf, inklusive bødekraft eller andre sanktioner, fra relevante myndigheder, samt krav fra øvrige tredjeparter, herunder de berørte datasubjekter, underdatabehandlere og databehandlerens øvrige samarbejdspartnere.

Vedr. Bestemmelse 7.3:

Den dataansvarlige anerkender, at databehandlerens Tjenester er standardiserede, cloud-baserede abonnementsydelser, der stilles til rådighed for et stort antal kunder, og at databehandleren derfor ikke har mulighed for at indrette de tilbudte systemer således, at hver kunde kan stille krav om, at databehandleren ikke må gøre brug af bestemte underdatabehandlere, som databehandleren i øvrigt har godkendt.

På den baggrund anerkender den dataansvarlige, at såfremt denne har indsigelser mod databehandlerens ændring eller valg af nye underdatabehandlere, og databehandleren ikke imødekommer sådan indsigelse, er den dataansvarliges eneste beføjelse at opsige abonnementsaftalen med databehandleren.

Opsigelsen kan ske med øjeblikkelig virkning, og ingen af parterne har nogen krav mod hinanden i anledning heraf.

Vedr. Bestemmelse 9.2:

I det omfang den dataansvarlige ønsker databehandlerens bistand til de ydelser, der er beskrevet under Bestemmelse 9.2, (c) og (d), er den dataansvarlige forpligtet til at vederlægge databehandleren for den herved anvendte tid med de af databehandleren til enhver tid anvendte timsatser, som fremgår på databehandlerens hjemmeside.

Vedr. Bestemmelse 12.1:

Databehandleren er forpligtet til at afsætte de ressourcer, der er nødvendig(e) for, at den dataansvarlige eller dennes rådgiver/repræsentant kan gennemføre sin inspektion og/eller revision hos databehandleren eller dennes underdatabehandlere. "Databehandlerens udgifter i forbindelse med en fysisk inspektion og/eller en på vegne den dataansvarlige udført revision hos databehandleren eller dennes underdatabehandlere, afholdes af den dataansvarlige. Databehandlerens og/eller dennes underdatabehandleres tid godtgøres med de af databehandleren til enhver tid anvendte timsatser, som fremgår på databehandlerens hjemmeside"

Vedr. Bestemmelse 13.1:

Databehandlerens ansvar overfor den dataansvarlige er begrænset til det i abonnementsbetingelserne anførte, ligesom de i abonnementsbetingelserne i øvrigt anførte bestemmelser finder anvendelse mellem den dataansvarlige og databehandleren, bortset fra i det omfang de forringer den registreredes grundlæggende rettigheder og frihedsrettigheder ifølge databeskyttelsesforordningen.