

Databehandleraftale

FieldTechie ApS · Version 2026-10-14

Hvad er det her?

Når I bruger FieldTechie, opbevarer og behandler vi personoplysninger for jer: jeres medarbejdere, jeres kunder og de personer, der optræder i jeres opgaver. I bestemmer over de oplysninger. Vi må kun gøre det, I beder os om.

Databeskyttelsesforordningen (GDPR) artikel 28 kræver, at det står i en skriftlig aftale. Det er denne aftale.

Hvad I får her

Del	Hvad det er
Parter (næste side)	Hvem aftalen er mellem. Vores oplysninger er udfyldt. Jeres felter er tomme
Bestemmelserne	Datatilsynets egen standardtekst (marts 2024), ord for ord. Vi har ikke ændret et komma
Bilag A	Hvilke personoplysninger vi behandler, om hvem, og hvor længe
Bilag B	De underleverandører, vi bruger, og hvad de får adgang til
Bilag C	Jeres instruks til os, og de sikkerhedsforanstaltninger vi har
Bilag D	Det, parterne aftaler derudover

Hvorfor Datatilsynets tekst? Tilsynet har selv vedtaget den som standardkontraktbestemmelser.

Bruger vi den uændret, behøver hverken I eller jeres rådgiver at gennemgå selve aftaleteksten. Det, der er værd at læse, er bilagene — og dem har vi skrevet så konkret som muligt.

Det korte overblik

- **Hvor ligger jeres data?** Hos Scaleway i Paris. Databasen er jeres egen, ikke en fælles.
- **Hvem andre rører dem?** De fire i Bilag B. Kort og adressesøgning kommer fra Google, og push-beskeder også — det står der, og vi påstår ikke, at alt ligger i EU.
- **Hvem hos os kan se dem?** I dag én person, og kun til drift og support.

- **Hvis noget går galt:** vi giver jer besked inden for 24 timer, efter vi har opdaget det. I har selv 72 timer til Datatilsynet.
- **Hvis I stopper:** I kan se alt og eksportere lister i 30 dage, og på anmodning sender vi jer en fuld kopi af alle jeres data. Derefter sletter vi det hele inden for 60 dage og bekræfter det skriftligt.
- **Sletning er rigtig sletning.** Vi markerer ikke bare data som slettede.

Hvad skal I gøre?

- **Accepterer I ved oprettelsen?** Så er aftalen indgået, når I sætter kryds ved abonnementsvilkårene. Vi gemmer tidspunkt, version og hvem der accepterede. I skal ikke underskrive noget.
- **Vil I have et underskrevet eksemplar?** Udfyld jeres felter på næste side, så sender vi det til underskrift.
- **Skal jeres egne medarbejdere vide noget?** Ja. Bruger I GPS-sporing eller tidsregistrering, er det jer, der skal informere jeres medarbejdere. Vi hjælper gerne med teksten.

Spørgsmål? Skriv til privacy@fieldtechie.com. I får svar fra et menneske, der har været med til at bygge systemet.

Standardkontraktsbestemmelser

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

mellem

Den dataansvarlige (kunden)

Navn

CVR-nr.

Adresse

Postnummer og by

Land

Kontaktperson for aftalen

Navn

Stilling

Telefon

E-mail

herefter "den dataansvarlige"

og

Databehandleren

Navn FieldTechie ApS

CVR-nr. 46686721

Adresse Mispelvej 1

Postnummer og by 9500 Hobro

Land Danmark

Kontaktperson for aftalen

Navn Lars Søgaard Jensen

Stilling Direktør

E-mail privacy@fieldtechie.com

herefter "databehandleren"

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

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

Ikrafttræden

Aftalen træder i kraft, når den dataansvarlige accepterer abonnementsvilkårene med tilhørende databehandleraftale ved oprettelsen, eller når begge parter har underskrevet nedenfor.

	Den dataansvarlige	Databehandleren
Navn		Lars Søgaard Jensen
Stilling		Direktør
Dato		
Underskrift		

Dette ark gengiver standardtekstens forside ordret, med parterne udfyldt. Det erstatter standardtekstens forside med de tomme partsfelter, ligesom Bilag A–D bagest erstatter de tomme bilagsskabeloner. Bestemmelserne på de følgende sider er gengivet uændret. Felterne til kontaktpersoner og underskrift i Bestemmelserne udfyldes på dette ark.

Changelog

VERSION	ÆNDRINGER
1.1	Ændringer i Bestemmelserne 7.7., 9.2., 10.4. og Bilag C.8. (<i>Tastefejl og opdaterede krydshenvisninger</i>).
1.2	Ændringer i Bestemmelse 7.6 (<i>Bestemmelsen er gjort valgfri og ordlyden er blevet modificeret</i>)

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.....	14
Bilag D Parternes regulering af andre forhold.....	19

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 **TJENESTE** 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.

[NOTE: PARTERNE BØR FORUDSE OG OVERVEJE KONSEKVENSERNE, DER KAN FØLGE AF EN POTENTIelt ULOVLIG INSTRUKS, SOM DEN DATAANSVARLIGE HAR GIVET OG REGULERE DETTE I EN AFTALE MELLEM PARTERNE.]

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 [VALG 1] specifik skriftlig godkendelse / [VALG 2] generel skriftlig godkendelse fra den dataansvarlige.
3. [VALG 1 FORUDGÅENDE SPECIFIK GODKENDELSE] Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst [ANGIV TIDSPERIODE] inden anvendelsen af den pågældende underdatabehandler. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

[VALG 2 FORUDGÅENDE GENEREL GODKENDELSE] 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 **[ANGIV TIDSPERIODE]** 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. **[VALGFRI]** Databehandleren skal i sin aftale med underdatabehandleren indføre den dataansvarlige som begunstiget tredjemand, således at den dataansvarlige i tilfælde af at databehandleren faktisk eller retligt set er ophørt med at eksistere eller i tilfælde af databehandlerens konkurs, har ret til at opsig underdatabehandleraftalen og 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 standardkontraktbestemmelser 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 indsigelse
 - j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til

behandlings 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, [ANGIV KOMPETENT TILSYNSMYNDIGHED], 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, [ANGIV KOMPETENT TILSYNSMYNDIGHED], 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 [ANTAL 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 [VALG 1] slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er slettet / [VALG 2] tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.
- 2. [HVIS RELEVANT] Følgende regler i EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne efter ophør af tjenesterne vedrørende behandling af personoplysninger:
 - a. [...]

Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

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 uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.
3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.
4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.
5. Underskrift

På vegne af den dataansvarlige

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

På vegne af databehandleren

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

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

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

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

Bilag A — Oplysninger om behandlingen

Behandlingen udgør én behandlingsaktivitet: levering af tjenesten FieldTechie til den dataansvarlige.

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

At levere tjenesten FieldTechie til den dataansvarlige i henhold til abonnementsvilkårene, herunder at:

- planlægge, fordele og dokumentere den dataansvarliges serviceopgaver;
- registrere arbejdstid og fravær;
- kommunikere med den dataansvarliges medarbejdere og kunder;
- fakturere og udveksle data med de regnskabs- og lønsystemer, som den dataansvarlige selv forbinder;
- yde support samt drive, sikre og tage backup af tjenesten.

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

- **Indsamling:**
- data indtastes af den dataansvarliges brugere eller indlæses fra filer;
- mobilappen registrerer GPS-positioner, mens en sporingssession er aktiv, samt fotos og underskrifter;
- data modtages fra systemer, som den dataansvarlige forbinder.
- **Opbevaring** hos Scaleway i Paris (fr-par): i en separat database for hver dataansvarlig, i objektlager og i backup, jf. Bilag C.2.
- **Organisering, søgning og visning** for den dataansvarliges brugere efter roller og rettigheder.
- **Automatisk anvendelse:**
- forslag til planlægning og beregning af ruter med en routingmotor, som databehandleren selv driver;
- pointgivning af teknikere som forslag til en disponent;
- automatisk sletning efter opbevaringsperioder.

Der træffes ingen automatiske afgørelser om de registrerede.

- **Videregivelse efter den dataansvarliges instruks eller konfiguration:**

- SMS- og e-mailbeskeder til den dataansvarliges kunder;
- push-beskeder til den dataansvarliges brugere;
- webhooks og eksport til systemer, som den dataansvarlige forbinder.
- **Sletning:** data slettes endeligt og markeres ikke blot som slettede.
- **Adgang for databehandlerens personale** alene til support og drift (jf. Bilag C).

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

1. Identitets- og kontaktoplysninger:

- navn, e-mail, telefonnummer og postadresse;
- stilling, virksomhed og afdeling;
- medarbejder- eller kontaktnummer.

For kontaktpersoner og medarbejdere desuden, hvis den dataansvarlige udfylder dem, fødselsdato og adresser på profiler på sociale medier. Hertil nærmeste pårørende til medarbejdere (navn, relation og kontaktoplysninger).

1. Brugerkonto og login:

- brugernavn, e-mail og brugeridentifikator;
- krypteret adgangskode og hemmelighed til engangskoder;
- sessioner og loghændelser for login, herunder IP-adresse (opbevares i 30 dage, jf. Bilag C.4);
- registrerede enheder og push-tokens;
- brugerindstillinger, roller og rettigheder;
- brugertype og aktiveringsperioder.

1. Planlægning og udførelse af arbejde:

- tildelte opgaver og aftaler med planlagte og faktiske tidspunkter for ankomst, start og slut;
- ruter;
- arbejdstidsplaner og vagter;
- kvalifikationer;
- kost- og timepriser;
- udleveret værktøj;
- point til forslag om tildeling af opgaver.

1. Arbejdstid og fravær:

- tidsregistreringer med bemærkninger;
- timesedler og godkendelser;
- fraværsanmodninger med den begrundelse, brugeren selv skriver.

1. **Lokalitet:**

- GPS-positioner (koordinater, nøjagtighed, højde, hastighed og retning) registreret af mobilappen, mens medarbejderen er stemplet ind, og den dataansvarlige har slået sporing til;
- senest kendte position;
- oplysninger om sporingssessioner (enhedsmodel, styresystem, tilbagelagt afstand, batteriniveau);
- GPS-oplysninger i fotos, medmindre de fjernes;
- koordinater for serviceadresser.

1. **Kommunikation:**

- chatbeskeder, herunder redigeringer;
- kanalmedlemskab og læsestatus;
- sagsbeskeder og interne beskeder;
- notifikationer i appen;
- beskeder til den dataansvarliges kunder (modtagerens telefonnummer eller e-mail, indhold og leveringsstatus);
- samtykke til og framelding af beskeder.

1. **Dokumentation:**

- fotos og filer;
- tjeklistesvar;
- håndskrevne underskrifter med underskriverens navn og rolle;
- noter og fritekstfelter, herunder felter, som den dataansvarlige selv opretter;
- servicehistorik;
- indlæste filer.

1. **Handelsoplysninger om enkeltmandsvirksomheder:**

- fakturaer og betalinger;
- CVR- og momsnummer;
- bankoplysninger.

1. Tekniske oplysninger og revisionsspor:

- log over, hvem der har ændret hvad, med tidligere og nye værdier;
- kopier af poster i tekniske beskeder (webhooks, jobs, import);
- koblinger til id'er i forbundne systemer;
- applikationslogs.

Helbredsoplysninger. Tjenesten leveres med fraværstyper for sygdom, lægebesøg, barsel og orlov af familie- eller helbredsmæssige årsager. Den dataansvarlige kan ændre disse typer. Registreres fravær af en sådan type for en medarbejder, behandles derfor oplysninger om medarbejderens helbred (databeskyttelsesforordningens artikel 9). Tjenesten beder ikke om diagnoser eller årsager til sygdom. Er et lønsystem forbundet, overføres fraværstype, dato og timer til det efter den dataansvarliges instruks.

Andre følsomme oplysninger og strafbare forhold. Tjenesten har ingen felter til andre følsomme oplysninger, fx fagforeningsmedlemskab, eller til oplysninger om strafbare forhold (artikel 10).

Personnumre (CPR). Databehandleren opbevarer ikke personnumre. Tjenesten har intet felt til personnummer, og fra forbundne lønsystemer læses kun medarbejdernummer, navn og e-mail. Medarbejdere matches på medarbejdernummer. Eneste undtagelse: en svensk enskild firmas organisationsnummer er ejerens personnummer og kan registreres som registreringsnummer for en kunde.

Fritekst, egne felter og fotos. Databehandleren kan ikke teknisk forhindre, at brugere skriver følsomme oplysninger eller personnumre i fritekstfelter, egne felter, chat eller fotos. Den dataansvarlige instruerer sine brugere i ikke at gøre det (jf. Bilag C).

A.4. Behandlingen omfatter følgende kategorier af registrerede

1. Den dataansvarliges brugere: ejer, kontorphonale, disponenter og ledere.
2. Den dataansvarliges teknikere og øvrige medarbejdere i marken, herunder lærlinge og underleverandørers medarbejdere med adgang til tjenesten.
3. Kontaktpersoner hos den dataansvarliges kunder.
4. Private kunder og beboere på de adresser, hvor der udføres service, samt enkeltmandsvirksomheder blandt den dataansvarliges kunder og leverandører.
5. Andre personer, som optræder i data: medarbejderes pårørende, underskrivere, inviterede brugere og personer i fotos eller fritekst.

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

Behandlingen har følgende varighed

Behandlingen varer, så længe den dataansvarliges abonnement løber, herunder prøveperioden. Derefter fortsætter den, indtil personoplysningerne er slettet eller tilbageleveret efter Bestemmelse 11 og Bilag C (læseadgang og eksport af lister i 30 dage og en fuld kopi på anmodning, sletning senest 60 dage efter ophør og udløb af backup inden for yderligere 14 dage, jf. Bilag C.4).

Bilag B — Underdatabehandlere

B.1. Godkendte underdatabehandlere

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

Navn	CVR / registreringsnr.	Adresse	Beskrivelse af behandling
Scaleway SAS	RCS Paris 433 115 904	8 rue de la Ville- l'Évêque, 75008 Paris, Frankrig	Hosting af hele tjenesten i Paris (fr-par): servere, databaser og backup, objektlager, cache, netværk, afsendelse af e-mails, logs og hemmeligheder. Omfatter alle typer personoplysninger i Bilag A. Behandlingen sker i EU.
Google LLC (Firebase Cloud Messaging)	Delaware-selskab (LLC), USA	1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Levering af push-beskeder til mobilappen: enhedens push-token samt beskedens titel og tekst. Kan behandles uden for EU; overførselsgrundlag: EU-US Data Privacy Framework (Google LLC er certificeret) og, som reserve, EU-Kommissionens standardkontraktbestemmelser i Firebases databehandlingsvilkår. Opbevaring: en notifikation, der ikke kan leveres med det samme, gemmes i op til 28 dage og kasseres derefter. På Android udløber en enheds registrering efter 270 dage uden brug; Google opbevarer app-installationens id, indtil det slettes, og fjerner det derefter inden for 180 dage.
Functional Software, Inc. (Sentry)	Delaware-selskab, USA	45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	Fejl- og nedbrudsrapporter fra mobilappen: oplysninger om enhed og app samt fejlens sammenhæng. Brugeridentitet sendes ikke. Data opbevares i Sentrys EU-region; overførselsgrundlag: EU-US Data Privacy Framework (Sentry er certificeret) og, som reserve, EU-Kommissionens standardkontraktbestemmelser i Sentrys databehandlertaftale. Opbevaring: fejlrapporter slettes efter højst 90 dage.

Navn	CVR / registreringsnr.	Adresse	Beskrivelse af behandling
ONLINECITY.IO ApS (GatewayAPI)	CVR 27364276	Buchwaldsgade 50, 5000 Odense C, Danmark	Afsendelse af SMS til den dataansvarliges kunder: modtagerens telefonnummer og beskeds tekst. Behandlingen sker i EU. Opbevaring: efter 30 dage anonymiseres beskedteksten, afsenderen og de sidste fire cifre i telefonnummeret. En sms, der er opkrævet ved en fejl, gemmes i 6 måneder til afregning af refusionen og anonymiseres derefter fuldt ud.

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.

Ikke underdatabehandlere: systemer, som den dataansvarlige selv forbinder (fx regnskabs- og lønsystemer og webhooks), er den dataansvarliges egne. Databehandleren sender dem kun data efter den dataansvarliges instruks. Software, som databehandleren selv driver hos Scaleway (brugerstyring, beskedkø, ruteberegning), er ikke underdatabehandlere. DNS for databehandlerens domæner leveres af Cloudflare, Inc. Trafikken til tjenesten går ikke gennem Cloudflare, og Cloudflare behandler ikke den dataansvarliges personoplysninger.

Modtager, der ikke er underdatabehandler: **Google Ireland Limited** (Google Maps Platform), 368047 (Irland), Gordon House, Barrow Street, Dublin 4, Irland. Når den dataansvarliges brugere bruger kort og addressesøgning, modtager Google:

- **ved adresseforslag og adresseopslag:** den adresse, brugeren skriver, sendt fra databehandlerens server;
- **ved kort og kortbilleder:** brugerens IP-adresse, det viste kortområde og, i kortbilleder, koordinater eller adressen på en kundes lokation, indlæst i brugerens browser.

Google behandler oplysningerne som **selvstændig dataansvarlig** efter Googles egne vilkår (Google Maps Platform og Googles Controller-Controller Data Protection Terms), ikke efter databehandlerens instruks. Google er derfor ikke underdatabehandler. Oplysningerne kan behandles uden for EU. Overførselsgrundlag: EU-Kommissionens standardkontraktbestemmelser (modul 1, mellem dataansvarlige) i Googles vilkår og EU-US Data Privacy Framework.

B.2. Varsel for godkendelse af underdatabehandlere

Den dataansvarlige giver en generel skriftlig forhåndsgodkendelse (Bestemmelse 7.3).

Varsel. Databehandleren varsler påtænkte tilføjelser eller udskiftninger af underdatabehandlere mindst **30 dage** før ændringen træder i kraft. Varslet sendes med e-mail til den dataansvarliges ejer og faktureringskontakt og offentliggøres på databehandlerens liste over underdatabehandlere.

Indsigelse. Den dataansvarlige kan inden for varslingsperioden gøre indsigelse af saglige databeskyttelsesmæssige grunde. Hvis ændringen alligevel gennemføres, kan den dataansvarlige opsige den berørte tjeneste uden omkostninger, inden ændringen træder i kraft.

Bilag C — Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

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

- **Levering af tjenesten.** Databehandleren leverer tjenesten FieldTechie som beskrevet i Bilag A og i abonnementsvilkårene. Det omfatter opbevaring, visning og bearbejdning af de personoplysninger, som den dataansvarliges brugere indtaster, indlæser eller registrerer via mobilappen.
- **Videregivelse.** Personoplysninger videregives kun til de systemer, modtagere og kanaler, som den dataansvarlige selv forbinder eller aktiverer i tjenesten, fx regnskabs- og lønsystemer, webhooks samt SMS- og e-mailbeskeder til kunder.
- **Support og drift.** Databehandleren tilgår kun personoplysningerne, når det er nødvendigt for drift, sikkerhed og fejlretning, eller når den dataansvarlige beder om support.
- **Den dataansvarliges ansvar.** Den dataansvarlige instruerer sine brugere i ikke at registrere følsomme oplysninger eller personnumre i fritextfelter, egne felter, chat eller fotos (jf. Bilag A.3). Den dataansvarlige informerer sine medarbejdere om GPS-sporing og registrering af arbejdstid.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle, at behandlingen er en almindelig erhvervstjeneste med to skærpende elementer:

- **Lokalitetsoplysninger** om den dataansvarliges medarbejdere (GPS-positioner og ruter).
- **Fraværstyper**, der kan afsløre helbredsforhold.

Behandlingen omfatter ikke en større mængde særlige kategorier af personoplysninger. Der etableres derfor et **normalt sikkerhedsniveau med skærpet beskyttelse af lokalitets-, fraværs- og adgangsdata**.

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

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

Pseudonymisering og kryptering

- **Adskillelse pr. kunde.** Hver dataansvarligs data opbevares i en separat database med sin egen databaserolle.
- **Kryptering af adgangsoplysninger.** Adgangsoplysninger til databaser, forbundne systemer og webhooks krypteres i applikationen med AES-256-GCM.
- **Nøgler.** Nøglerne opbevares i Scaleway Secret Manager og er kun tilgængelige for driftsserverne.

Fortrolighed, integritet, tilgængelighed og robusthed

- **Adgangskontrol.** Brugernes adgang styres af roller og rettigheder pr. handling og datatype. Hver forespørgsel knyttes til kunden ud fra brugerens medlemskab, som slås op på serveren. Kunde-id i forespørgslen accepteres ikke.
- **Automatiske tests.** Kundeadskillelsen er dækket af automatiske tests, som køres ved hver ændring.
- **Drift.** Tjenesten drives bag en load balancer med sundhedstjek. Beskeder mellem tjenestens dele gemmes, før de sendes, så et nedbrud forsinker dem uden at tabe dem.

Genopretning efter hændelser

- **Backup.** Databaserne sikkerhedskopieres automatisk én gang i døgnet som et øjebliksbillede af hele databaseserveren, så alle dataansvarliges databaser er med. Hver kopi opbevares i **14 dage** hos Scaleway i Paris (fr-par). Genopretning af en enkelt dataansvarligs database følger en skriftlig procedure, som er afprøvet.

Regelmæssig afprøvning og evaluering

- **Tests.** Automatiske tests af sikkerhedskritiske funktioner (kundeadskillelse, cookies, CORS, HTTPS) køres ved hver ændring. Kun afprøvede versioner kan sættes i drift.
- **Hemmeligheder i kode.** Koden scannes for hemmeligheder ved hver ændring.
- **Sårbarheder og opdateringer.** Afhængigheder skannes løbende for kendte sårbarheder, og styresystemer og containere opdateres jævnligt.
- **Evaluering.** Foranstaltningerne i dette bilag gennemgås mindst én gang om året, og når tjenesten ændres væsentligt.

Adgang til oplysningerne via internettet

- **Login.** Brugere logger ind via databehandlerens egen login-tjeneste (Keycloak):
 - adgangskoder på mindst 12 tegn;
 - spærring efter gentagne forkerte forsøg;
 - bekræftelse af e-mail;
 - adgangstokens med 5 minutters gyldighed.
- **To-faktor-godkendelse** tilbydes alle brugere. Den dataansvarlige opfordres til at kræve det for ejere og administratorer.
- **Databehandlerens personale.** Personale med administrativ adgang skal bruge to-faktor-godkendelse. Administrationsadgang er ikke åben mod internettet og sker kun via krypteret forbindelse fra godkendte adresser.

Beskyttelse af oplysninger under transmission

- **Kryptering.** Al trafik mellem brugere og tjenesten krypteres med TLS, og HTTP omdirigeres til HTTPS.
- **E-mail.** E-mails sendes krypteret til e-mailtjenesten.
- **Internt netværk.** Intern trafik mellem tjenestens servere sker i Scaleways private netværk, som ikke er tilgængeligt fra internettet.
- **Database.** Forbindelsen til databasen er krypteret, og databasens certifikat verificeres.
- **Webhooks.** Webhooks sendes kun via HTTPS og signeres. Adresser i private netværk afvises.

Beskyttelse af oplysninger under opbevaring

- **Kryptering på disk.** Databaserne er krypteret på disk hos Scaleway.
- **Adgangsoplysninger** er desuden krypteret i applikationen (se ovenfor).
- **Sletning.** Data slettes endeligt og markeres ikke blot som slettede.
- **Mobilappen.** Loginoplysninger gemmes i enhedens sikre lager. Data, som appen gemmer til brug uden netforbindelse, er ikke krypteret ud over enhedens egen kryptering. Den dataansvarlige sørger for, at enhederne er beskyttet med skærmlås.

Fysisk sikring af lokaliteter

Behandlingen sker udelukkende i Scaleways datacentre i Paris-regionen (fr-par). Fysisk sikring varetages af Scaleway i henhold til underdatabehandleraftalen. Databehandleren opbevarer ikke personoplysninger på egne lokaliteter.

Hjemme-/fjernarbejdspladser

Databehandlerens personale arbejder fra hjemme- og fjernarbejdspladser. Adgang til driftsmiljøet sker kun via krypterede forbindelser og personlige, to-faktor-beskyttede konti. Personoplysninger kopieres ikke til personalets egne enheder, bortset fra hvad support af en konkret sag kræver, og slettes derefter. Arbejdsstationer med adgang har krypteret disk og automatisk skærmlås.

Logning

- **Ændringer.** Alle ændringer af den dataansvarliges data logges med bruger, tidspunkt og tidligere og nye værdier.
- **Login og administration.** Loginhændelser og administrative hændelser i login-tjenesten opbevares i 30 dage.
- **Applikationslogs** opbevares i op til 31 dage, samlet i Scaleway Cockpit i Paris.
- **Visninger.** Hvem der har læst hvilke oplysninger, logges ikke.

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:

- **Anmodninger fra registrerede (selvbetjening).** Den dataansvarliges brugere kan selv se, rette og slette oplysninger om registrerede i tjenesten.
- **Hvad databehandleren sletter eller udtrækker.** Oplysninger, som ikke kan håndteres ved selvbetjening, sletter eller udtrækker databehandleren inden for **10 arbejdsdage** efter skriftlig anmodning fra den dataansvarlige. Det gælder kopier i logs, tekniske beskeder og indlæsninger.
- **Betaling.** Bistanden er uden beregning, medmindre anmodningerne er åbenbart overdrevne.
- **Konsekvensanalyser og forudgående høring.** Databehandleren stiller Bilag A–C og sin sikkerhedsbeskrivelse til rådighed, herunder en skabelon til konsekvensanalyse for lokalitetssporing. Databehandleren besvarer rimelige spørgsmål inden for **10 arbejdsdage**.
- **Brud på persondatasikkerheden.** Databehandleren underretter den dataansvarlige uden unødigt forsinkelse og senest **24 timer** efter at være blevet bekendt med bruddet, jf. Bestemmelse 10.2, med de oplysninger, der kendes på tidspunktet, og supplerer, efterhånden som undersøgelsen skrider frem.

C.4 Opbevaringsperiode/sletterutine

Under abonnementet opbevares personoplysninger, indtil den dataansvarlige sletter dem, med følgende automatiske sletning:

- **Chatbeskeder:** 24 måneder som standard. Den dataansvarlige kan ændre perioden.
- **Rå GPS-positioner:** 90 dage som standard. Den dataansvarlige kan ændre perioden.
- **Log over ændringer:** 24 måneder.
- **Webhook-leveringer og -hændelser:** 30 hhv. 90 dage.
- **Log- og administrationshændelser** i login-tjenesten: 30 dage.
- **Applikationslogs:** 31 dage.
- **Backup:** 14 dage.

Ved ophør af tjenesten vedrørende behandling af personoplysninger tilbageleverer databehandleren personoplysningerne og sletter derefter eksisterende kopier, jf. Bestemmelse 11.1:

- **Eksport.** Tjenesten er tilgængelig i læsetilstand i **30 dage** efter ophør, så den dataansvarlige selv kan se alle oplysninger og eksportere lister. På den dataansvarliges anmodning inden for de 30 dage udleverer databehandleren en **fuld kopi af alle oplysninger, inklusive filer**, i et almindeligt anvendt, maskinlæsbart format, senest 10 arbejdsdage efter anmodningen og altid inden sletningen.
- **Sletning.** Derefter slettes den dataansvarliges database, filer, brugere og brugerkonti inden for yderligere **30 dage**. Alt er således slettet fra driftssystemerne senest 60 dage efter ophør.
- **Backup.** Slettede oplysninger forsvinder fra backup, efterhånden som den udløber, senest **14 dage** efter sletningen.
- **Bekræftelse.** Databehandleren bekræfter sletningen skriftligt på anmodning.
- **Kopier hos underdatabehandlere.** Kopier hos underdatabehandlere (sms, push-notifikationer og fejlrapporter) slettes efter de opbevaringsperioder, der står i Bilag B.
- **Prøveperiode.** En prøveperiode, der ikke fortsætter som abonnement, slettes 30 dage efter udløbet af den efterfølgende læseperiode på 14 dage. Den dataansvarlige advares forinden to gange på e-mail.

Dette gælder, medmindre den dataansvarlige – efter accepten af disse Bestemmelser – har ændret sit oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til Bestemmelserne.

Databehandlerens egne oplysninger. Databehandlerens egne oplysninger om den dataansvarlige som kunde behandles af databehandleren som dataansvarlig og er ikke omfattet af Bestemmelse 11:

- **Fakturaer, kreditnotaer og betalinger:** opbevares i 5 år efter regnskabsårets udløb efter bogføringsloven.
- **Dokumentation for accept af aftalen:** opbevares i 5 år efter ophør.

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:

- **Scaleway SAS:** datacentre i Paris-regionen (fr-par), Frankrig. Hosting af hele tjenesten, herunder backup.
- **Databehandlerens personale:** hjemme- og fjernarbejdspladser i Danmark. Administration og support, jf. C.2.
- **Øvrige underdatabehandlere** som angivet i Bilag B, for den dér beskrevne behandling.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Den dataansvarlige instruerer databehandleren i at overføre personoplysninger til tredjelande i følgende tilfælde og kun i det omfang, det er beskrevet i Bilag B:

- **Push-beskeder:** Google (Firebase Cloud Messaging).
- **Kort og adressesøgning:** videregivelse til Google Maps Platform, når brugerne bruger kort og adressesøgning. Google modtager oplysningerne som selvstændig dataansvarlig (Bilag B, modtager, der ikke er underdatabehandler) og overfører dem efter Googles egne vilkår: EU-Kommissionens standardkontraktbestemmelser, modul 1 (mellem dataansvarlige), og EU-US Data Privacy Framework. Kort indlæses i brugerens browser.
- **Fejlrapporter fra mobilappen:** Sentry, kun hvis data ikke kan holdes i Sentrys EU-region.

Overførselsgrundlag (databeskyttelsesforordningens kapitel V):

- **Hovedgrundlag:** Europa-Kommissionens afgørelse om tilstrækkeligt beskyttelsesniveau for EU-US Data Privacy Framework (artikel 45) for de modtagere, der er certificeret.
- **Supplerende grundlag:** Europa-Kommissionens standardkontraktbestemmelser (artikel 46, stk. 2, litra c) i underdatabehandlernes vilkår.

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

- **Årlig erklæring.** Databehandleren sender én gang om året uden beregning en skriftlig erklæring fra sin ledelse til den dataansvarlige. Erklæringen omfatter overholdelsen af disse Bestemmelser og Bilag C samt en oversigt over sikkerhedsforanstaltningerne og ændringer siden sidste erklæring.
- **Spørgeskema.** Databehandleren besvarer desuden ét sikkerhedsspørgeskema fra den dataansvarlige om året uden beregning.
- **Yderligere revision.** Den dataansvarlige kan derudover for egen regning gennemføre en revision eller inspektion. Følgende gælder:
 - den varsles mindst **30 dage** i forvejen og sker inden for normal arbejdstid under tavshedspligt;
 - den gennemføres som udgangspunkt uden fysisk fremmøde, medmindre den dataansvarlige begrundet behovet for mere;
 - den giver ikke adgang til andre kunders oplysninger.
- **Datacentre.** Fysisk inspektion af datacentre er ikke mulig. Den er dækket af underdatabehandlerens certificeringer, jf. C.8.
- **Uden for aftalen.** Revisionserklæringer efter ISAE 3000/3402 og ISO 27001-certificering af databehandleren er ikke omfattet af aftalen.
- **Anfægtelse.** Den dataansvarlige kan anfægte rammerne for og metoden i erklæringen og anmode om yderligere oplysninger.

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

- **Årlig gennemgang.** Databehandleren gennemgår én gang om året hver underdatabehandleres offentliggjorte certificeringer og revisionserklæringer samt ændringer i dennes databehandleraftale.
- **Opsummering.** På anmodning sender databehandleren en opsummering til den dataansvarlige.
- **Ingen fysisk inspektion.** Databehandleren foretager ikke fysiske inspektioner hos underdatabehandlerne, som alle leverer standardiserede tjenester.

Bilag D — Parternes regulering af andre forhold

D.1 Forholdet til abonnementsvilkårene

Disse Bestemmelser regulerer behandlingen af personoplysninger. Alt andet — pris, betaling, aftaleperiode, opsigelse, tilgængelighed og ansvar — følger abonnementsvilkårene, som Bestemmelserne er bilag til.

Ved uenighed om behandling af personoplysninger går Bestemmelserne og bilagene forud for abonnementsvilkårene.

D.2 Indgåelse og dokumentation

Aftalen indgås, når den dataansvarlige accepterer abonnementsvilkårene med tilhørende databehandleraftale ved oprettelsen af sin konto.

Databehandleren registrerer og opbevarer **tidspunktet, den accepterede version af hvert dokument og hvem der accepterede**. Den dataansvarlige kan til enhver tid få en kopi af registreringen og af de accepterede dokumenter.

Et særskilt underskrevet eksemplar kan aftales og ændrer ikke aftalens indhold.

D.3 Ændringer af Bestemmelserne og bilagene

- **Varsel.** Databehandleren varsler ændringer mindst **30 dage** før de træder i kraft, med e-mail til den dataansvarliges ejer og kontaktperson.
- **Undtagelse.** Ændringer, der alene gengiver ændringer i lovgivningen eller i Datatilsynets standardtekst, kan gennemføres uden varsel. Den dataansvarlige orienteres.
- **Indsigelse.** Den dataansvarlige kan gøre indsigelse inden ikrafttræden af saglige databeskyttelsesmæssige grunde. Kan parterne ikke blive enige, kan den dataansvarlige opsige abonnementet uden omkostninger inden ændringens ikrafttræden.
- **Underdatabehandlere** varsles efter Bilag B.2.

D.4 Valgfrie bestemmelser, som parterne ikke har aftalt

- **Bestemmelse 7.6** (den dataansvarlige som begunstiget tredjemand i databehandlerens aftaler med underdatabehandlere) **er ikke aftalt**. Databehandlerens underdatabehandlere leverer

standardiserede tjenester på egne vilkår, som ikke kan ændres for den enkelte kunde.

D.5 Sprog

Bestemmelserne og bilagene findes på dansk og engelsk. **Den danske udgave går forud** ved uoverensstemmelse. Den engelske udgave er en oversættelse til brug for læsere, der ikke læser dansk.

D.6 Kontakt

Henvendelser om denne aftale, om anmodninger fra registrerede og om brud på persondatasikkerheden sendes til databehandlerens kontaktperson på forsiden. Den dataansvarlige oplyser databehandleren om ændringer i sin egen kontaktperson.

D.7 Felter og valg i Bestemmelserne

Bestemmelserne er Datatilsynets standardtekst og gengives uændret. Felterne og valgene i teksten udfyldes således:

- **Bestemmelse 2.3** [TJENESTE]: tjenesten **FieldTechie**, jf. Bilag A.
- **Bestemmelse 7.2–7.3** [VALG 1] / [VALG 2]: **Valg 2**, generel skriftlig forhåndsgodkendelse. Varslet [ANGIV TIDSPERIODE] er **30 dage**, jf. Bilag B.2.
- **Bestemmelse 7.6** [VALGFRI]: ikke aftalt, jf. D.4.
- **Bestemmelse 9.2** [ANGIV KOMPETENT TILSYNSMYNDIGHED]: **Datatilsynet**.
- **Bestemmelse 10.2** [ANTAL TIMER]: **24 timer**, jf. Bilag C.3.
- **Bestemmelse 11.1** [VALG 1] / [VALG 2]: **Valg 2**: databehandleren tilbageleverer personoplysningerne og sletter derefter eksisterende kopier, jf. Bilag C.4.
- **Bestemmelse 11.2** [HVIS RELEVANT]: **ingen**. Hverken EU-retten eller dansk ret kræver, at databehandleren opbevarer den dataansvarliges personoplysninger efter ophøret.
- **Bestemmelse 14 og 15** (underskrift og kontaktpersoner): udfyldes på partsarket forrest i aftalen.