

Mit Beredskab ApS

Databehandleraftale

Version 2.0

Gældende fra 18.09.2026

Parter

Databehandler

Mit Beredskab ApS

CVR-nr. 42299529

Niels Jernes Vej 10, 9220 Aalborg Øst

kontakt@mitberedskab.dk

Dataansvarlig

Udfyldes ved accept

Om denne aftale

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

1. Parter

Denne databehandleraftale er indgået mellem den dataansvarlige og databehandleren, der hver især er en part og sammen udgør parterne.

Den dataansvarlige

Felt	Oplysning
Virksomhed eller myndighed	Udfyldes ved accept
CVR-nr.	Udfyldes ved accept
Adresse	Udfyldes ved accept
Land	Udfyldes ved accept

Databehandleren

Felt	Oplysning
Virksomhed eller myndighed	Mit Beredskab ApS
CVR-nr.	42299529
Adresse	Niels Jernes Vej 10, 9220 Aalborg Øst
Land	Danmark

Parterne har aftalt følgende med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med leveringen af Mit Beredskab.

2. Præambel

- 2.1. Denne aftale fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.
- 2.2. Denne aftale 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).
- 2.3. I forbindelse med leveringen af Mit Beredskab behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med denne aftale.
- 2.4. Denne aftale har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
- 2.5. Denne aftale erstatter enhver tidligere databehandleraftale mellem parterne fra det

tidspunkt, hvor den dataansvarlige accepterer den.

- 2.6. Der hører fire bilag til denne aftale, og bilagene udgør en integreret del af aftalen.
- 2.7. 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.
- 2.8. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
- 2.9. 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.
- 2.10. Bilag D indeholder den information, som databehandleren skal stille til rådighed ved brud på persondatasikkerheden, jf. bestemmelse 10.4.
- 2.11. Aftalen med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
- 2.12. Denne aftale frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Den dataansvarliges rettigheder og forpligtelser

- 3.1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og denne aftale.
- 3.2. 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.
- 3.3. 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

- 4.1. 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 denne aftale.
- 4.2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5. Fortrolighed

- 5.1. 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.
- 5.2. Databehandleren er, under og efter denne aftales ophør, pålagt fuld tavshedspligt omkring alle oplysninger, denne bliver bekendt med gennem samarbejdet. Aftalen indebærer, at tavshedspligtsbestemmelserne i straffelovens §§ 152-152f, jf. straffelovens § 152a, finder anvendelse.
- 5.3. Databehandleren skal sikre, at alle, der behandler oplysninger omfattet af denne aftale, herunder ansatte, tredjeparter og underdatabehandlere, forpligter sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.
- 5.4. Databehandleren må ikke hverken offentligt eller til tredjeparter kommunikere om brud på persondatasikkerheden uden forudgående skriftlig aftale med den dataansvarlige om indholdet af en sådan kommunikation, medmindre databehandleren har en retlig forpligtelse til sådan kommunikation.
- 5.5. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

- 6.1. 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.
- 6.2. 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:
 - pseudonymisering og kryptering af personoplysninger
 - evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
 - evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
 - en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.
- 6.3. 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.

- 6.4. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32 ved blandt andet 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.
- 6.5. 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

- 7.1. 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).
- 7.2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af denne aftale uden forudgående generel skriftlig godkendelse fra den dataansvarlige.
- 7.3. 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 90 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.
- 7.4. 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 denne aftale, 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 denne aftale og databeskyttelsesforordningen.
- 7.5. Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter denne aftale og databeskyttelsesforordningen.
- 7.6. 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 denne aftale er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen,

skal ikke sendes til den dataansvarlige.

- 7.7. 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

- 8.1. 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.
- 8.2. 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.
- 8.3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af denne aftale:
- overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
 - overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
 - behandle personoplysningerne i et tredjeland
- 8.4. 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.
- 8.5. Denne aftale skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og denne aftale kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

9. Bistand til den dataansvarlige

- 9.1. 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.
- 9.2. Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:
- oplysningspligten ved indsamling af personoplysninger hos den registrerede
 - oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede

- indsigtsretten
 - retten til berigtigelse
 - retten til sletning (retten til at blive glemt)
 - retten til begrænsning af behandling
 - underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
 - retten til dataportabilitet
 - retten til indsigelse
 - retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
- 9.3. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til bestemmelse 6.4 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.
- 9.4. 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 9.3.

10. Underretning om brud på persondatasikkerheden

- 10.1. Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
- 10.2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 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.
- 10.3. I overensstemmelse med bestemmelse 9.3.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:
- 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
 - de sandsynlige konsekvenser af bruddet på persondatasikkerheden
 - 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.
- 10.4. Parterne skal i bilag D 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.
- 10.5. Databehandleren skal føre en oversigt over samtlige brud på persondatasikkerheden.

11. Sletning og returnering af oplysninger

- 11.1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger sletter databehandleren den dataansvarliges tenant i Mit Beredskab. Dermed slettes tenanten, dens workspaces og alt, der hører til dem, jf. oversigten i bilag A.3. Databehandleren bekræfter skriftligt over for den dataansvarlige, at sletningen er gennemført.
- 11.2. Sletningen af tenanten omfatter ikke brugerkonti. En brugerkonto tilhører brugeren selv og kan være medlem af flere tenants, så den består, når tenanten slettes. Brugeren kan selv slette sin konto, og den dataansvarlige kan bede databehandleren om at slette navngivne konti, hvorefter databehandleren sletter dem.
- 11.3. Sletningen omfatter heller ikke revisionsposter og fejllogge. De opbevares i de perioder, der fremgår af bilag C.4, og slettes derefter automatisk.
- 11.4. Sletningen omfatter endelig ikke rettighedssæt og tildelte rettigheder knyttet til den slettede tenant eller dens workspaces. De slettes ikke automatisk, fordi de er optegnelsen over, hvem der har haft adgang til tenanten. De indeholder identifikatorer for, hvem der oprettede dem, og hvem de var tildelt, og databehandleren sletter dem efter anmodning fra den dataansvarlige.
- 11.5. Medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne, slettes alt øvrigt som beskrevet ovenfor.

12. Revision, herunder inspektion

- 12.1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og denne aftale, 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.
- 12.2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i bilag C.7.
- 12.3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivning 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

- 13.1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om for eksempel erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod aftalen eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

14. Ikrafttræden og ophør

- 14.1. Aftalen træder i kraft på datoen for begge parters underskrift heraf. Databehandleren underskriver ved at udgive versionen, og den dataansvarlige underskriver ved at acceptere aftalen i Mit Beredskab.
- 14.2. Denne udgave er version 2.0 med virkning fra 18.09.2026. Udgaven er kendetegnet ved kontrolsummen 60d639dfe8776775f96606d7f8bc6b298e3dfb60b774539b23702d36455bb7f7, der dækker de oplysninger om behandlingen, som aftalen gengiver.
- 14.3. Begge parter kan kræve aftalen genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i aftalen giver anledning hertil.
- 14.4. Aftalen er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan aftalen ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.
- 14.5. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet i overensstemmelse med bestemmelse 11.1 og bilag C.4, kan aftalen opsiges med skriftligt varsel af begge parter.

15. Kontaktpersoner hos den dataansvarlige og databehandleren

Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

På vegne af den dataansvarlige:

Felt	Oplysning
Navn	Udfyldes ved accept
Stilling	Udfyldes ved accept
Telefonnummer	Udfyldes ved accept
E-mail	Udfyldes ved accept

På vegne af databehandleren:

Felt	Oplysning
Navn	Anders Udengaard Bischoff
Stilling	Direktør

Felt	Oplysning
Telefonnummer	+45 73 70 87 01
E-mail	kontakt@mitberedskab.dk

Databehandleren har ikke udpeget en databeskyttelsesrådgiver.

Bilag A - Oplysninger om behandlingen

Bilaget beskriver den behandling af personoplysninger, som databehandleren foretager på vegne af den dataansvarlige.

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

Behandlingen har til formål at levere Mit Beredskab til den dataansvarlige og de brugere, den dataansvarlige opretter. Databehandleren må ikke anvende oplysningerne til andre formål, og personoplysninger må ikke behandles efter instruks fra andre end den dataansvarlige. De enkelte formål fremgår af nedenstående oversigt; behandlingsgrundlaget fastlægges af den dataansvarlige, jf. bestemmelse 3.3.

Oplysninger	Formål
Handlekort	at de handlekort, personalet skal følge, kan holdes ét sted
Kvitteringer for handlekort	at det kan dokumenteres, at en person har kvitteret for en bestemt version af et handlekort
Kladder til handlekort	at et handlekort kan skrives færdigt, før det udgives
Visninger af handlekort	at det kan dokumenteres, hvem der har set eller hentet et handlekort, og hvornår
Beskeder om handlekort	at den, der har et handlekort, får besked, når der kommer en ny version
Udgivne handlekort	at en udgivet version af et handlekort kan genfindes, som den så ud dengang
Adresser	at en tenant eller et workspace kan stedsfæstes på en adresse
Accepterede databehandleraftaler	at det kan dokumenteres, hvilken version af databehandleraftalen den dataansvarlige har accepteret, og hvornår
Alarmhændelser	at en alarmhændelse kan dokumenteres og efterprøves bagefter
Alarmgrupper	at et workspace kan sætte op, hvem der kaldes i hvilken alarm
Positioner under en alarm	at det kan ses, hvor den enkelte responder befandt sig undervejs, så indsatsen kan følges og efterprøves bagefter
Udkald på en alarm	at det kan dokumenteres, hvem der blev kaldt i hvilken bølge, og om beskeden nåede frem
Svar på en alarm	at det kan dokumenteres, hvem der svarede på en alarm, hvordan og hvor hurtigt

Oplysninger	Formål
API-nøgler	at et system kan få adgang til tjenesten med sin egen nøgle i stedet for med en persons login
Samlingssteder	at de kaldte kan sendes til det rette samlingssted
Revisionslog	at det kan efterprøves bagefter, hvem der udførte en privilegeret handling, og hvad der skete
Øvelser	at en øvelse kan planlægges og gennemføres, og at det kan dokumenteres, hvem der var ansvarlig og hvem der deltog
Evalueringer af øvelser	at erfaringerne fra en øvelse kan skrives ned og bruges næste gang
Forløbet af en øvelse	at det kan gengives skridt for skridt, hvem der gjorde hvad hvornår i en øvelse
Opfølgningspunkter	at et opfølgningspunkt efter en øvelse kan tildeles, følges og lukkes
Påmindelser om øvelser	at den ansvarlige bliver mindet om en øvelse eller et opfølgningspunkt
E-mailadresser	at en tenant eller et workspace kan nås på e-mail
Kvitteringer for udsendt e-mail	at det kan efterprøves, om en udsendt e-mail nåede frem til den enkelte modtager
Fejllog	at en fejl kan findes og rettes for den bruger, den ramte
Filer	at en bruger, et workspace eller en tenant kan lægge filer op og hente dem igen
Gruppemedlemskaber	at en adgang kan gives til en gruppe i stedet for til hver enkelt person
Bekræftelseslinks	at en følsom handling kan bekræftes gennem et link sendt til brugeren, før den udføres
Invitationer	at en person kan inviteres ind i en tenant, og at det kan ses, hvem der inviterede og hvem der accepterede
Medlemskaber	at det kan afgøres og dokumenteres, hvem der er til stede i en tenant eller et workspace, og hvorfor
Beskeder i tjenesten	at en bruger kan modtage og genfinde beskeder inde i tjenesten
Rettighedssæt	at rettigheder kan samles i et sæt, der kan tildeles i en tenant eller et workspace
Telefonnumre	at en bruger, en tenant eller et workspace kan nås på telefon
Bilag til dokumenter	at en fil kan vedhæftes et dokument og genfindes sammen med det
Beredskabsdokumenter	at et workspace eller en tenant kan holde sine beredskabsdokumenter samlet ét sted
Kvitteringer for dokumenter	at det kan dokumenteres, at en person har kvitteret for en bestemt version af et dokument

Oplysninger	Formål
Udgivne beredskabsdokumenter	at en udgivet version af et dokument kan genfindes, som den så ud dengang
Påmindelser om dokumenter	at den ansvarlige bliver mindet om et dokument, der skal gennemgås eller kvitteres
Svar på krav	at det kan dokumenteres, om et krav gælder her, og hvem der svarede på det
Tildelte rettigheder	at et rettighedssæt kan tildeles en bestemt identitet, og at det kan ses, hvem der tildelte det
Identitet i adgangsstyringen	at en bruger, en gruppe eller en applikation kan kendes fra hinanden i adgangsstyringen
Kvitteringer for alarmbeskeder til telefoner	at det kan ses, om en alarmbesked nåede frem til en telefon, og at den samme kvittering kun kan bruges én gang
Enheder, der modtager push-beskeder	at en besked kan leveres som push til brugerens egne enheder
Aktive logins	at en bruger kan se og afslutte sine egne aktive logins på hver enhed
Tenantens stamdata	at en tenant kan kontaktes og faktureres
Brugerkonto	at en person kan få adgang til tjenesten og kan kontaktes i den
Adgangskode	at en brugers adgangskode kan kontrolleres, når personen logger ind
Brugerindstillinger	at tjenesten kan vises og give besked på den måde, den enkelte bruger har valgt
Workspacets stamdata	at et workspace kan kontaktes gennem den person, den dataansvarlige har udpeget

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

Behandlingen består i indsamling, registrering, opbevaring, brug, videregivelse til de underdatabehandlere, der fremgår af bilag B, og sletning af personoplysninger i Mit Beredskab.

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

Oversigten er dannet ud fra de dataerklæringer, platformens moduler afgiver om deres egne tabeller, så den beskriver det, systemet faktisk gemmer.

Oplysninger	Kategorier af personoplysninger	Beskrivelse	Opbevaring
Handlekort	hvem der oprettede handlekortet, og hvem der sidst ændrede det	hvem der oprettede et handlekort, og hvad kortet dækker; beskrivelsen er fritekst og kan nævne personer	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.

Oplysninger	Kategorier af personoplysninger	Beskrivelse	Opbevaring
Kvitteringer for handlekort	hvem der har kvitteret for hvilken version af et handlekort, og hvornår	dokumentation for at en person har kvitteret for en bestemt version af et handlekort	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Kladder til handlekort	hvem der skriver på kladden, og hvornår den sidst blev gemt	hvem der sidst rettede i kladden, og deres note om ændringen; noten er fritekst og kan nævne personer	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Visninger af handlekort	hvem der har åbnet eller hentet hvilket handlekort, og hvornår	hvem der så eller hentede et handlekort, og hvornår	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Beskeder om handlekort	hvem der fik besked om en ny version af et handlekort, og hvornår	hvem der blev adviseret om en ny version af et handlekort	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Udgivne handlekort	hvem der udgav versionen, og hvornår	hvem der udgav en version af et handlekort, og deres note om ændringen; noten er fritekst og kan nævne personer	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Adresser	gade, postnummer, by, land, geografisk position og en fritekstnote, der kan nævne personer	delt adresse med position, som en tenant eller et workspace peger på; noten er fritekst og kan nævne personer	Slettes sammen med ejeren, som oplysningen hører til.
Accepterede databehandleraftaler	navn og e-mailadresse på den, der accepterede, og hvilken klient der blev brugt	dokumentation for indgået databehandleraftale: hvem accepterede hvilken version, hvornår og fra hvilken klient	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Alarmhændelser	navnet på den, der udløste alarmen, dennes besked, og samlingsstedets navn og position	dokumentation af alarmhændelser: hvem udløste alarmen, hvornår, med hvilken besked og hvor mødestedet lå	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Alarmgrupper	hvem der oprettede gruppen, og hvilke medlemmer der kaldes i den	opsætning af en alarmgruppe i et workspace, og hvem der oprettede den	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Positioner under en alarm	navnet på responderen og dennes geografiske position med nøjagtighed, mens alarmen er aktiv	dokumentation af alarmhændelser: hvor responderen befandt sig undervejs, så indsatsen kan følges og efterprøves	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Udkald på en alarm	hvem der blev kaldt i hvilken bølge, og om beskeden nåede frem	dokumentation af alarmhændelser: hvem blev kaldt i hvilken bølge, på hvilken telefon, og hvad der blev målt om udsendelsen	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Svar på en alarm	navnet på den, der svarede, hvad vedkommende svarede, og hvornår	dokumentation af alarmhændelser: hvem svarede på alarmen, hvordan og hvor hurtigt	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
API-nøgler	hvilken identitet en nøgle tilhører, hvem der udstedte den, og hvornår den sidst blev brugt	at et system kan få adgang med sin egen nøgle i stedet for med en persons login	Slettes sammen med ejeren, som oplysningen hører til.
Samlingssteder	den geografiske position på et samlingssted	positionen på et samlingssted i et workspace, som responderne sendes til	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.

Oplysninger	Kategorier af personoplysninger	Beskrivelse	Opbevaring
Revisionslog	hvem der handlede, e-mailadresse, IP-adresse, browser eller app, og hvad handlingen ændrede	revisionsspor: hvem gjorde hvad, hvornår og hvorfra, så en handling kan efterprøves	Revisionsloggen slettes efter 730 dage.
Øvelser	hvem der planlagde øvelsen, hvem der deltog, og hvornår den blev holdt	dokumentation af en øvelse: hvem var ansvarlig, hvem deltog, hvad blev observeret undervejs, og hvorfor den eventuelt blev aflyst; scenariet, det frosne alarmbillede og aflysningsgrunden er fritekst og kan nævne personer	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Evalueringer af øvelser	hvem der skrev evalueringen, og fritekst om forløbet, der kan nævne personer	evalueringen efter en øvelse, og hvem der udfyldte den; felterne er fritekst og kan nævne personer	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Forløbet af en øvelse	hvem der gjorde hvad undervejs i øvelsen, og hvornår	tidslinjen for en øvelse: hvem gjorde hvad hvornår, med den frie note der hører til	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Opfølgningspunkter	hvem et opfølgningspunkt er tildelt, hvem der oprettede det, og hvornår det blev lukket	opfølgningspunkter efter en øvelse: hvem der skal handle, hvem der lukkede punktet, og begrundelsen	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Påmindelser om øvelser	hvem der blev mindet om en øvelse eller et opfølgningspunkt, og hvornår	hvem der blev mindet om en øvelse eller et opfølgningspunkt	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
E-mailadresser	e-mailadresse	delt e-mailadresse, som en tenant eller et workspace peger på	Slettes sammen med ejeren, som oplysningen hører til.
Kvitteringer for udsendt e-mail	modtagerens e-mailadresse og de oplysninger, beskeden blev flettet med	leveringsoptegnelse for en udsendt e-mail, så det kan efterprøves om beskeden nåede frem	Kvitteringer for udsendt e-mail slettes efter 90 dage.
Fejllog	e-mailadresse, IP-adresse, browser eller app, og fritekst fra fejlen, der kan nævne personer	fejlsøgning: hvilken anmodning fejlede, for hvem, så fejlen kan findes og rettes; stacksporet er fritekst og kan nævne personer	Fejlloggen slettes 90 dage efter, at fejlen er lukket, og 730 dage efter, at den opstod, hvis den stadig er åben.
Filer	filnavn, hvem der lagde filen op, og hvem den tilhører	filer ejet af en bruger, et workspace eller en tenant, og hvem der lagde dem op	Slettes sammen med ejeren, som oplysningen hører til.
Gruppemedlemskaber	hvilken identitet der er medlem af hvilken gruppe, og hvem der tilføjede den	at en adgang kan gives til en gruppe i stedet for til hver enkelt person	Slettes sammen med ejeren, som oplysningen hører til.
Bekræftelseslinks	et engangslink i hashet form og oplysningerne om den handling, der skal bekræftes, for eksempel et skift af e-mailadresse	bekræftelse af en følsom handling gennem et link sendt til brugeren	Slettes senest efter 31 dage.
Invitationer	navn og e-mailadresse på den inviterede, hvem der inviterede, og en personlig besked	invitation af en person til en tenant, og optegnelsen af hvem der inviterede og hvem der accepterede	Invitationer slettes efter 90 dage.
Medlemskaber	hvem der er medlem af hvilken tenant eller hvilket workspace, hvem der inviterede dem, og en note om hvorfor	medlemskab, tildeling og operatøradgang: hvem der er til stede i en tenant eller et workspace, og hvorfor	Slettes sammen med ejeren, som oplysningen hører til.

Oplysninger	Kategorier af personoplysninger	Beskrivelse	Opbevaring
Beskeder i tjenesten	beskedens overskrift og tekst, og om den er læst	beskeder til brugeren i platformen, og om de er læst	Notifikationer slettes efter 90 dage.
Rettighedssæt	navnet på et sæt af rettigheder og hvem der oprettede det	at rettigheder kan samles i et sæt, der kan tildeles i en tenant eller et workspace	Oplysninger uden fastsat frist opbevares, indtil de slettes manuelt; der sker ingen automatisk sletning.
Telefonnumre	telefonnummer med landekode	delt telefonnummer, som en tenant, et workspace eller en brugerprofil peger på	Slettes sammen med ejeren, som oplysningen hører til.
Bilag til dokumenter	filnavn og hvem der vedhæftede filen	hvem der vedhæftede en fil til et dokument	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Beredskabsdokumenter	hvem der oprettede dokumentet, og hvem der er ansvarlig for det	hvem der oprettede et dokument i myndighedsmappen, og selve dokumentets tekst; beskrivelsen og det udgivne udkast er fritext og kan nævne personer	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Kvitteringer for dokumenter	hvem der har kvitteret for hvilken version af et dokument, og hvornår	dokumentation for at en person har kvitteret for en bestemt version af et dokument	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Udgivne beredskabsdokumenter	hvem der udgav versionen, og hvornår	hvem der udgav en version, og noten om hvad der blev ændret; noten er fritext og kan nævne personer	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Påmindelser om dokumenter	hvem der blev mindet om et dokument, og hvornår	hvem der blev mindet om et dokument, der skal gennemgås eller kvitteres	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Svar på krav	hvem der svarede på, om et krav gælder her, og hvornår	hvem der svarede på om et krav gælder for dette workspace, og noten til svaret; noten er fritext og kan nævne personer	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Tildelte rettigheder	hvilken identitet et rettighedssæt er tildelt, og hvem der tildelte det	at et rettighedssæt kan tildeles en bestemt identitet, og at det kan ses, hvem der tildelte det	Oplysninger uden fastsat frist opbevares, indtil de slettes manuelt; der sker ingen automatisk sletning.
Identitet i adgangsstyringen	navn på identiteten og en henvisning til den bruger, gruppe eller applikation, den står for	at en bruger, en gruppe eller en applikation kan kendes fra hinanden i adgangsstyringen	Slettes sammen med ejeren, som oplysningen hører til.
Kvitteringer for alarmbeskeder til telefoner	et tilfældigt id for den enkelte besked, og hvornår kvitteringen blev givet	kvittering for at en alarmbesked nåede frem til en telefon, og at den samme kvittering kun kan bruges én gang	Slettes senest efter 1 dag.
Enheder, der modtager push-beskeder	enhedens navn og platform, appens version og sprog, og en teknisk nøgle, der leverer beskeden til enheden	levering af push-beskeder til brugerens egne enheder	Slettes, når brugeren slettes.
Aktive logins	IP-adresse, enhedsmodel, styresystem og et navn på enheden	aktive logins, så brugeren kan se og afslutte sine egne sessioner på hver enhed	Udløber efter 3650 dages inaktivitet (mobilapp) og 365 dages inaktivitet (browser).

Oplysninger	Kategorier af personoplysninger	Beskrivelse	Opbevaring
Tenantens stamdata	kontakt- og faktureringsoplysninger, herunder en navngiven fakturakontakt	kontakt- og faktureringsoplysninger for en tenant, og hvem der bad om at få den slettet	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.
Brugerkonto	navn, e-mailadresse og en henvisning til brugerens telefonnummer	brugerens identitet og kontaktoplysninger, så personen kan logge ind og modtage beskeder	Slettes, når brugeren slettes.
Adgangskode	adgangskode i hashet form	kontrol af adgangskode ved login	Slettes, når brugeren slettes.
Brugerindstillinger	valg af sprog og tema, og hvilke notifikationer brugeren vil have	brugerens eget sprogvalg, så platformen skriver til personen på det sprog	Slettes, når brugeren slettes.
Workspacets stamdata	kontaktoplysninger, herunder en navngiven kontaktperson	kontaktoplysninger for et workspace, herunder den navngivne kontaktperson	Slettes sammen med den tenant eller det workspace, som oplysningen hører til.

Platformen har ingen felter til særlige kategorier af personoplysninger (artikel 9), til oplysninger om straffedomme og lovovertrædelser (artikel 10) eller til CPR-numre, og databehandleren indsamler dem ikke. Enkelte felter er fritekst og udfyldes af den dataansvarliges egne brugere efter den dataansvarliges instruks; den dataansvarlige instruerer dem i ikke at skrive sådanne oplysninger i dem.

A.4. Behandlingen omfatter følgende kategorier af registrerede

- ansatte hos den dataansvarlige, der er oprettet som brugere i tjenesten
- eksterne medarbejdere og konsulenter hos den dataansvarlige, der er oprettet som brugere i tjenesten
- kontaktpersoner og fakturakontakter, som den dataansvarlige angiver for en tenant eller et workspace

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

Behandlingen varer, så længe den dataansvarlige anvender Mit Beredskab. Ved ophør slettes oplysningerne som beskrevet i bilag C.4.

Bilag B - Underdatabehandlere

Bilaget angiver de underdatabehandlere, den dataansvarlige har godkendt brugen af.

B.1. Godkendte underdatabehandlere

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

Navn	Behandling	Lokation	Overførsel til tredjelande
Decree ApS (CVR-nr. 46410122)	Udvikling, drift og hosting af platformen	Danmark	Ingen overførsel til tredjelande (EU/ EØS)

Navn	Behandling	Lokation	Overførsel til tredjelande
Scaleway SAS	Hosting af platformens API, database og webklient, objektlagring af brugerfiler, udsendelse af e-mail	Frankrig (fr-par)	Ingen overførsel til tredjelande (EU/EØS)
Google LLC	Firebase Cloud Messaging: levering af push-beskeder til appens enheder	USA	EU-U.S. Data Privacy Framework
Apple Inc.	Apple Push Notification service: levering af push-beskeder til iOS-enheder	USA	Europa-Kommissionens standardkontraktbestemmelser, jf. databeskyttelsesforordningens artikel 46, stk. 2, litra c

Push-beskeder kan ikke sendes uden om Googles og Apples egne tjenester på deres enheder. Der findes i dag intet EU-alternativ. Skulle et opstå, vil vi vurdere et skifte.

Ved aftalens 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

Databehandleren underretter den dataansvarlige om en tilføjelse eller udskiftning af en underdatabehandler med mindst 90 dages varsel, jf. bestemmelse 7.3. Underretningen sker ved, at databehandleren udgiver en ny version af denne aftale i Mit Beredskab med en ikrafttrædelsesdato mindst 90 dage frem, og at den dataansvarliges ejer får besked i Mit Beredskab ved næste logind. Den dataansvarlige kan gøre indsigelse inden for varsløst.

B.3. Modtagere, som brugerens egen enhed kontakter direkte

Kortet i webklienten og i mobilappen henter kortfliser hos nedenstående tjenester. Anmodningen sendes af brugerens egen browser eller enhed, og tjenesten modtager enhedens IP-adresse og det kortudsnit, der vises. Databehandleren har ingen aftale med disse tjenester og videregiver ingen oplysninger til dem, og bestemmelse 7.4 til 7.7 omfatter dem derfor ikke.

Navn	Behandling	Lokation	Overførsel til tredjelande
OpenStreetMap Foundation	Levering af kortfliser til webklientens kort; modtager den besøgendes IP-adresse	Storbritannien	Europa-Kommissionens tilstrækkelighedsafgørelse for Det Forenede Kongerige, jf. databeskyttelsesforordningens artikel 45, gældende til 27. december 2031
OpenFreeMap	Levering af kortfliser til mobilappens kort; modtager enhedens IP-adresse	Oplyses ikke af leverandøren	Ikke oplyst

Bilag C - Instruks vedrørende behandling af personoplysninger

Bilaget er den dataansvarliges instruks til databehandleren.

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren stiller Mit Beredskab til rådighed, opretter og administrerer de brugere, den dataansvarlige beder om, og behandler de oplysninger, brugerne afgiver i tjenesten, med det formål, der fremgår af bilag A.

C.2. Behandlingssikkerhed

Databehandleren er 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:

- Forbindelsen fra platformens API til den administrerede database er krypteret med TLS, og databasens eget certifikat er den eneste betroede rod for forbindelsen.
- Platformens udgående e-mail sendes over en SMTP-forbindelse, der er beskyttet med TLS fra forbindelsens første byte, uden opgradering undervejs.
- Hver funktion i platformens API erklærer en autorisationsregel, og koden kan ikke bygges, hvis erklæringen mangler dér, hvor funktionen defineres.
- Der skrives en revisionslog over privilegerede handlinger, og et dagligt job sletter poster, der er ældre end den opbevaringsperiode, der fremgår af C.4.
- Automatisk backup er slået til på den administrerede databaseinstans.
- Versionering er slået fra på det objektlager, brugernes filer ligger i, så en slettet fil fjernes og ikke efterlader en genskabelig version.
- Når en bruger, et workspace eller en tenant slettes, efterlades alene en revisionspost, der viser hvad der blev slettet, af hvem og hvornår, og som for en bruger bevarer personens e-mailadresse. Der gemmes ingen kopi af den slettede post, tredjeparter, der mistede adgang, angives alene ved identifikator, og kontaktoplysninger, herunder telefonnummer, e-mailadresse og adresse, slettes sammen med den, de hører til.

Opbevaringsperioder og sletterrutiner fremgår af C.4.

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 9.3 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

- adgang for den dataansvarliges administratorer til logoplysninger om deres egne brugeres handlinger
- logoplysninger, der kan bidrage til kortlægning over et hændelsesforløb, herunder dets omfang og varighed
- tidslinje over forløbet
- beskrivelse af årsag til og karakteren af et brud
- hvilke mitigerende handlinger databehandleren har foretaget, og hvilke den dataansvarlige bør foretage
- hvilke mitigerende tiltag der planlægges, for at hændelsen ikke forekommer igen
- hvis relevant, hvilke teknologier der har været involveret.

C.4. Opbevaringsperiode/sletterutine

Personoplysninger opbevares i Mit Beredskab efter følgende perioder:

- Oplysninger, der hører til en bruger, slettes, når brugeren slettes.
- Oplysninger, der hører til en tenant eller et workspace, slettes sammen med den tenant eller det workspace, som oplysningen hører til.
- Oplysninger, der peger på en ejer, slettes sammen med ejeren.
- En session fra en browser udløber efter 365 dages inaktivitet.
- En session fra mobilappen udløber efter 3650 dages inaktivitet. Telefonen er den enhed, en alarm skal nå frem til, så den forbliver logget ind, og 3650 dage er platformens maksimum.
- Oplysninger til bekræftelse af en følsom handling gennem et link sendt til brugeren slettes senest efter 31 dage.
- Oplysninger til kvittering for at en alarmbesked nåede frem til en telefon, og at den samme kvittering kun kan bruges én gang slettes senest efter 1 dag.
- Fejlloggen slettes 90 dage efter, at fejlen er lukket, og 730 dage efter, at den opstod, hvis den stadig er åben.
- Invitationer slettes efter 90 dage.
- Kvitteringer for udsendt e-mail slettes efter 90 dage.
- Notifikationer slettes efter 90 dage.
- Revisionsloggen slettes efter 730 dage.
- Oplysninger uden fastsat frist opbevares, indtil de slettes manuelt; der sker ingen automatisk sletning.

Ved aftalens ophør igangsætter databehandleren sletningen uden unødigt forsinkelse, jf. bestemmelse 11.1. Platformen gennemfører sletningen efter et varslingsforløb på 30 dage, hvor tenantens ejer varsles; forløbet forlænges, hvis den sidste varslings ikke har kunnet afsendes. Databehandleren bekræfter skriftligt, når sletningen er gennemført. Parterne kan skriftligt aftale andet.

C.5. Lokalitet for behandling

Behandling af de af aftalen omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

- databehandlerens forretningsadresse, Niels Jernes Vej 10, 9220 Aalborg Øst
- hjemmearbejdspladser hos databehandlerens medarbejdere
- platformens driftsmiljø hos Scaleway SAS i Paris, Frankrig (regionen fr-par)
- de lokaliteter, der fremgår af bilag B.1

C.6. Instruks vedrørende overførsel af personoplysninger til tredjelande

Følgende underdatabehandlere overfører personoplysninger til tredjelande på det angivne grundlag:

Modtager	Land	Overførselsgrundlag
Google LLC	USA	EU-U.S. Data Privacy Framework
Apple Inc.	USA	Europa-Kommissionens standardkontraktbestemmelser, jf. databeskyttelsesforordningens artikel 46, stk. 2, litra c

Følgende modtagere, som brugerens egen enhed kontakter direkte, behandler oplysninger i et tredjeland på følgende grundlag:

Modtager	Land	Overførselsgrundlag
OpenStreetMap Foundation	Storbritannien	Europa-Kommissionens tilstrækkelighedsafgørelse for Det Forenede Kongerige, jf. databeskyttelsesforordningens artikel 45, gældende til 27. december 2031

Følgende modtagere oplyser ikke, hvor de behandler oplysningerne. Databehandleren kan ikke fastslå, om der sker overførsel til et tredjeland, og den dataansvarlige instrueres ikke i en sådan overførsel:

Modtager	Behandling	Hvad leverandøren oplyser
OpenFreeMap	Levering af kortfliser til mobilappens kort; modtager enhedens IP-adresse	Leverandøren oplyser ikke, hvor kortfliserne serveres fra.

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

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

Den dataansvarlige eller en repræsentant for den dataansvarlige kan med mindst 30 dages varsel foretage en fysisk inspektion af de lokaliteter, hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen, med henblik på at fastslå databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og denne aftale.

Ud over det planlagte tilsyn kan den dataansvarlige gennemføre en inspektion hos databehandleren, når den dataansvarlige finder det nødvendigt.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer, hovedsageligt den tid, der er nødvendige for, at den dataansvarlige kan gennemføre sin inspektion.

Bilag D - Informationer der skal stilles til rådighed ved brud på persondatasikkerheden

Databehandleren underretter den dataansvarlige om et brud på persondatasikkerheden inden for den frist, der fremgår af bestemmelse 10.2. Databehandleren stiller derefter vederlagsfrit nedenstående oplysninger til rådighed uden unødigt forsinkelse og i takt med, at de bliver tilgængelige, jf. databeskyttelsesforordningens artikel 33, stk. 4:

- logoplysninger, der kan bidrage til kortlægning over hændelsesforløbet, herunder til kortlægning over omfanget og varigheden af hændelsen
- tidslinje over forløbet
- beskrivelse af årsag til og karakteren af bruddet
- hvilke mitigerende handlinger databehandleren har foretaget, og hvilke mitigerende handlinger den dataansvarlige bør foretage
- hvilke mitigerende tiltag der planlægges, for at hændelsen ikke forekommer igen
- hvis relevant, hvilke teknologier der har været involveret.

Underskrifter

Databehandler

Mit Beredskab ApS

CVR-nr. 42299529

Anders Udengaard Bischoff, Direktør

Underskrevet ved udgivelse den 18.09.2026

Dataansvarlig

Udfyldes ved accept

Revisionsoversigt

Dokumenthistorik

Nedenfor står hver udgave af aftalen, datoen den trådte i kraft, hvad der blev ændret, og om ændringen er væsentlig eller redaktionel. En væsentlig ændring kræver, at den dataansvarlige accepterer aftalen på ny.

Version	Dato	Ændring	Type
2.0	18.09.2026	Ny aftale for den nye platform; erstatter tidligere aftaler	Væsentlig