Standardkontraktsbestemmelser

i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger
Version 12 – opdateret 23. november 2026

mellem
[Organisationens navn]

CVR [organisationens CVR-nummer]
[Adresse]
Danmark

herefter ”den dataansvarlige”

og

Center For Social Nytænkning, v. Steffen Rasmussen
CVR-nr.: 29561575
Nørreport 26D, 2., 8000 Aarhus C
Danmark

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

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 systemet NGO Basen (et webbaseret CRM-system til foreninger) 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 af 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 medlemsstaternes[1] nationale ret og disse Bestemmelser.

[1] Henvisninger til "medlemsstat" i disse bestemmelse skal forstås som en henvisning til "EØS medlemsstater".

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

4. Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.

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

5. Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.

2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

   Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

   a. Pseudonymisering og kryptering af personoplysninger

b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.

3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

   Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).

2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.

3.

   Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

   Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

6. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:

   a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
   b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
   c. behandle personoplysningerne i et tredjeland

4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.

5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

9. Bistand til den dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

   Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

   a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
   b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
   c. indsigtsretten
   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 behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

   a. den dataansvarliges forpligtelse til uden unødig 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 unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig 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 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.

3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

   a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

   b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

   c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er slettet eller – hvis den dataansvarlige anmoder herom – tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-

retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

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. Procedurerne 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:
   Stilling:
   Telefonnummer:

E-mail:

Underskrift

På vegne af databehandleren
Navn: Steffen Rasmussen
Stilling: Indehaver
Telefonnummer: 26195278
E-mail: steffen@cfsn.dk

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.

Den dataansvarlige:
Navn:
Stilling:
Telefonnummer:
E-mail:

Databehandleren:
Navn: Steffen Rasmussen
Stilling: Indehaver
Telefonnummer: 26195278
E-mail: steffen@cfsn.dk

Bilag A Oplysninger om behandlingen

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

Formålet med behandlingen er, at databehandleren stiller systemet NGO Basen til rådighed for den dataansvarlige. NGO Basen er et webbaseret CRM-system til administration af medlemmer, borgere, frivillige, donationer, fundraising, nyhedsbreve, møder, kalender og lokalebooking. Behandlingen sker alene med det formål at levere, drifte og vedligeholde systemet for den dataansvarlige.

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

Behandlingen består i opbevaring, organisering, visning, redigering, sletning og eksport af de personoplysninger, som den dataansvarlige og dennes brugere indtaster eller importerer i NGO Basen, samt afsendelse af e-mails (fx nyhedsbreve, invitationer og kvitteringer) på den dataansvarliges anvisning. Databehandleren foretager desuden fejlretning, support og sikkerhedskopiering som led i driften af systemet. AI-hjælp ved import: Når den dataansvarliges brugere importerer filer, kan dele af filens indhold sendes til en AI-tjeneste (OpenAI via Lovable) for at genkende kolonner, skelne private medlemmer fra virksomheder og læse teksten i PDF-eksporter af medlemmer, donationer og frivillige, jf. Bilag C.1 og C.6.

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

Almindelige personoplysninger: navn, adresse, e-mailadresse, telefonnummer, fødselsdato, profilbillede, medlemskabstype, betalingsoplysninger (beløb og betalingsstatus), donationer, kategori-/holdtilhørsforhold, pårørende og kontaktpersoner, samtykker, mødedeltagelse, fravær (datoer), noter uden følsomt indhold og vedhæftede filer.
CPR-numre.
Oplysninger i journalnotater, logbogsindlæg, personnoter, indskrivningssamtaler, dagbogsnotater og fraværsårsager, som kan omfatte følsomme oplysninger efter databeskyttelsesforordningens artikel 9, herunder helbredsoplysninger, samt fortrolige oplysninger om sociale forhold. Oplysningerne kan vedrøre personer i sårbare situationer, herunder unge under 18 år. CPR-numre og disse oplysninger opbevares adskilt fra systemets øvrige data, jf. Bilag C.2. Journalnotater og andre noter om deltagerne kan også indeholde oplysninger om strafbare forhold, jf. databeskyttelsesforordningens artikel 10 og databeskyttelseslovens § 8. Disse oplysninger opbevares på samme måde i den separate database.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Den dataansvarliges deltagere (som den dataansvarlige selv kan kalde fx elever, borgere eller beboere), herunder unge under 18 år, medlemmer (private og virksomheder), frivillige, medarbejdere og praktikanter, bestyrelsesmedlemmer, donorer, nyhedsbrevsmodtagere, pårørende og kontaktpersoner samt deltagere i møder og lokalebookinger.

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

Behandlingen påbegyndes ved Bestemmelsernes ikrafttræden og varer, så længe den dataansvarlige har en aktiv konto i NGO Basen. Ved aftalens ophør slettes eller returneres personoplysningerne i overensstemmelse med Bestemmelse 11 og Bilag C.4.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	SELSKAB	STED	BESKRIVELSE AF BEHANDLING
Lovable Labs Incorporated (Lovable Cloud)	Lovable Labs Incorporated, 1111b South Governors Avenue, Dover, DE 19904, USA. Intet CVR. DPO: dpo@lovable.dev. Direkte underdatabehandler.	Database og filer: Frankfurt, Tyskland (EU)	Hosting og drift af applikationen og den almindelige database, herunder login og fillagring, afsendelse af systemets e-mails og AI-hjælp ved import. Lovable anvender selv de underdatabehandlere, der er nævnt nedenfor. Databehandleren har en databehandleraftale med Lovable, jf. teksten under tabellen.
Supabase Pte. Ltd. (pengeskabet)	Supabase Pte. Ltd., 65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513. Reg.nr. 202005760H (Singapore), intet CVR. Direkte underdatabehandler.	London, Storbritannien (AWS eu-west-2)	Hosting af den separate, krypterede database til CPR-numre og følsomme oplysninger, jf. Bilag C.2. Databehandlerens egen konto på Supabases Pro-abonnement.
Supabase (via Lovable)	Via Lovable (andet led). Intet CVR; adresse i Lovables liste.	Frankfurt, Tyskland (EU)	Database, login og fillagring for den almindelige database.
Cloudflare, Inc. (via Lovable)	Via Lovable (andet led). Intet CVR; adresse i Lovables liste.	Globalt netværk	Afvikling af serverfunktioner og levering af websiden. Data i transit.
Mailgun (via Lovable)	Via Lovable (andet led).	USA	Afsendelse af systemets e-mails (fx invitationer, kvitteringer og

NAVN	SELSKAB	STED	BESKRIVELSE AF BEHANDLING
	Intet CVR; adresse i Lovables liste.		nyhedsbreve, når den dataansvarlige ikke selv har koblet Mailchimp på).
OpenAI (via Lovable AI Gateway)	Via Lovable (andet led). Intet CVR; adresse i Lovables liste.	USA	AI-hjælp ved import af filer, alene med de oplysninger, der er beskrevet i Bilag C.1: kolonneoverskrifter og højst 8 eksempelrækker uden CPR-numre, ved medlemsimport kun navn, firmanavn, CVR og medlemstype, tekst fra PDF-eksporter af medlemmer, donationer og frivillige (PDF'er med CPR-numre afvises) samt budgetfiler. Borgere kan ikke importeres via PDF. CPR-numre og oplysninger fra den separate database sendes aldrig.

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.
Rækkerne mærket "via Lovable" er underdatabehandlere, som Lovable anvender i leveringen af NGO Basen. Lovables fulde og til enhver tid gældende liste findes i Lovables Trust Center på trust.lovable.dev/subprocessors (rækkerne ovenfor er senest gennemgået 13. november 2026). Supabases liste over egne underdatabehandlere (bl.a. Amazon Web Services) findes på supabase.com. Databehandleren har en databehandleraftale med Lovable Labs Incorporated. Aftalen følger med Lovables Business-abonnement, som databehandleren har haft siden 14. september 2026, og er en del af Lovables vilkår (Lovables databehandleraftale, senest opdateret 17. november 2025 og underskrevet af Lovable 24. november 2025). Aftalen gælder, så længe databehandleren er på Lovables Business- eller Enterprise-abonnement. Efter aftalen skal Lovable ved kontrakt pålægge sine underdatabehandlere de samme databeskyttelsesforpligtelser, og Lovable må ikke bruge personoplysningerne til at træne AI-modeller. Lovable Labs Incorporated og Supabase Pte. Ltd. er databehandlerens direkte underdatabehandlere. Rækkerne mærket "via Lovable" er Lovables egne underdatabehandlere (underdatabehandlere i andet led), som Lovable efter sin databehandleraftale er ansvarlig for. Aftalen med Supabase Pte. Ltd. er Supabases databehandleraftale (Data Processing Addendum), som supplerer og er en del af Supabases vilkår. Ingen af underdatabehandlerne er danske selskaber, og de har derfor intet CVR-nummer; deres registreringsoplysninger er angivet i tabellen.

B.2. Varsel for godkendelse af underdatabehandlere

Databehandleren giver skriftligt varsel om tilføjelse eller udskiftning af underdatabehandlere senest 30 dage før ændringen. Gør den dataansvarlige saglig indsigelse, kan den dataansvarlige opsige aftalen om brug af NGO Basen med virkning fra ændringens ikrafttræden.

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:

Databehandleren stiller NGO Basen til rådighed, opbevarer og behandler de oplysninger, den dataansvarlige registrerer eller importerer, udfører de funktioner, den dataansvarliges brugere aktiverer i systemet (fx udsendelse af nyhedsbreve, invitationer og kvitteringer, import og eksport), yder support og fejlretning samt sletter oplysninger efter den dataansvarliges anvisning. AI-hjælp ved import sker kun, når en bruger selv vælger at importere en fil, og omfatter alene: (a) kolonneoverskrifter og højst 8 eksempelrækker til genkendelse af kolonner, hvor CPR-numre er erstattet med teksten "[CPR fjernet]", før de sendes; (b) ved import af medlemmer alene kolonnerne med navn, firmanavn, CVR-nummer og medlemstype, så private medlemmer kan skelnes fra virksomheder – adresser, kontaktoplysninger, beløb og noter sendes ikke; (c) teksten i en PDF-eksport af medlemmer, donationer eller frivillige; teksten læses på brugerens egen computer, og indeholder den et CPR-nummer, afvises filen, før noget sendes, og selve PDF-filen sendes aldrig; (d) budgetfiler ved import af budgetter. Borgere (fx fra Viggo) kan ikke importeres fra PDF og læses derfor uden AI-hjælp. CPR-numre, journalnotater og andre oplysninger fra den separate database sendes aldrig til AI-tjenesten.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Behandlingen omfatter CPR-numre og oplysninger, som kan være omfattet af databeskyttelsesforordningens artikel 9, om personer i sårbare situationer, herunder unge under 18 år. Der er derfor fastsat et højt sikkerhedsniveau.

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

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

1. Adskillelse. CPR-numre, journalnotater, logbogsindlæg, personnoter, indskrivningssamtaler, dagbogsnotater og fraværsårsager opbevares i en separat database (pengeskabet), adskilt fra applikationens øvrige data. Applikationens almindelige database afviser at gemme disse oplysninger.

2. Kryptering ved opbevaring. Hver værdi i den separate database krypteres på applikationsniveau med AES-256-GCM og en unik, tilfældig initialiseringsvektor, før den gemmes. Krypteringsnøglen opbevares adskilt fra databasen og er kun tilgængelig for applikationens server. Underdatabehandlerne krypterer desuden alle data og sikkerhedskopier ved opbevaring.

3. Integritet. Hver krypteret værdi er kryptografisk bundet til den dataansvarliges organisation, den konkrete post (fx personen) og det konkrete felt, så den ikke kan læses, hvis den flyttes til en anden række eller organisation.

4. Kryptering under transport. Al kommunikation mellem bruger, applikation og databaser sker over krypterede forbindelser (HTTPS/TLS).

5. Adgangsstyring. Den separate database kan ikke tilgås fra brugerens browser eller med offentlige nøgler. Adgang sker udelukkende gennem applikationens server efter login, og før

en oplysning udleveres, kontrolleres det, at brugeren tilhører den dataansvarliges organisation og har ret til at se den. Hver organisations data er logisk adskilt med adgangsregler på rækkeniveau. Roller opbevares i en særskilt beskyttet tabel, og den dataansvarliges administratorer styrer, hvilke dele af systemet brugerne har adgang til. CPR-numre kan kun ses af administratorer. Adgangskoder opbevares alene i hashet form, og integrationsnøgler kan kun læses af serveren.

6. Logning. Hver visning og gemning af en oplysning i den separate database logges med bruger, tidspunkt, handling, post og felt (for fritekstfelter felttypen). Loggen indeholder ikke selve oplysningen og opbevares, så længe aftalen løber. Øvrige følsomme handlinger, fx ændring af integrationer og sletning, registreres i en audit-log, som brugerne ikke kan ændre eller slette.

7. Fejlhåndtering. Kan en oplysning ikke krypteres eller dekrypteres, afvises handlingen, og brugeren får en fejlbesked. Oplysninger gemmes aldrig ukrypteret som alternativ, og krypteret tekst vises aldrig for brugeren.

8. Adgang hos databehandleren og underdatabehandlerne. Hos databehandleren har kun Steffen Rasmussen adgang til drifts- og databasekonti. Kontiene er beskyttet med tofaktorgodkendelse. Databehandleren tilgår kun den dataansvarliges oplysninger efter dokumenteret instruks, fx ved support og fejlretning, og kun via sikrede forbindelser. Underdatabehandlerne har teknisk adgang i det omfang, deres ydelse kræver det: Lovable som platform kan teknisk tilgå den almindelige database og filerne, og når databehandleren udvikler og fejlretter systemet med Lovables AI-udviklingsværktøj, kan værktøjet på databehandlerens anvisning læse oplysninger i den almindelige database. Applikationens server kører hos Lovable (på Cloudflares netværk), og krypteringsnøglen til den separate database opbevares der som en hemmelig servernøgle; CPR-numre og følsomme oplysninger passerer derfor krypteret over netværket og ukrypteret i serverens hukommelse, når en bruger med adgang ser eller gemmer dem, men de gemmes ikke hos Lovable. Supabase kan teknisk tilgå den separate database, men kun se krypterede værdier.

9. Filer. Vedhæftede filer og profilbilleder opbevares i et lukket fillager uden offentlig adgang og kan kun hentes via tidsbegrænsede links af brugere med adgang.

10. Backup. Den almindelige database sikkerhedskopieres automatisk én gang i døgnet hos Lovable Cloud, og kopierne opbevares i op til ca. 14 dage. Vedhæftede filer er ikke omfattet af disse sikkerhedskopier. Pengeskabet ligger hos Supabase på Pro-abonnementet (Pro Plan) i London (eu-west-2) og sikkerhedskopieres automatisk én gang i døgnet. Ifølge Supabases dokumentation kan projekter på Pro-abonnementet bruge de seneste 7 dages daglige sikkerhedskopier (kilde: supabase.com/docs/guides/platform/backups, set 13. november 2026). Point-in-Time Recovery (et tillæg med løbende sikkerhedskopiering) er ikke slået til. Filer i pengeskabets fillager (Storage) er ikke omfattet af sikkerhedskopierne. Sikkerhedskopier er krypteret hos underdatabehandlerne.

11. Test og opfølgning. Databehandleren gennemfører løbende sikkerhedsscanninger af systemet, afprøver adskillelsen mellem organisationer og retter fund uden unødig forsinkelse.

12. Fysisk sikring. Den fysiske sikring af serverlokaliteter varetages af underdatabehandlerne. Databehandleren har ingen egne serverlokaliteter.

13. Begrænsninger. Krypteringen sker på serveren og ikke hos den enkelte bruger, så systemet er ikke ende-til-ende-krypteret. Databehandleren er ikke selv certificeret efter ISO 27001.

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:

Systemet giver den dataansvarlige mulighed for selv at søge, rette, eksportere og slette oplysninger om den enkelte registrerede, så anmodninger om indsigt, berigtigelse, sletning og dataportabilitet kan håndteres af den dataansvarlige selv.

Kan en anmodning ikke håndteres via systemets funktioner, bistår databehandleren efter skriftlig anmodning og inden for en frist, der gør det muligt for den dataansvarlige at svare den registrerede inden for 1 måned. Modtager databehandleren en anmodning direkte fra en registreret, videresendes den uden unødig forsinkelse til den dataansvarlige, og databehandleren besvarer den ikke selv.

Brud på persondatasikkerheden (Bestemmelse 9.2.a–b og 10.4): Databehandleren underretter den dataansvarliges kontaktperson, jf. Bestemmelse 15, og organisationens administratorer i NGO Basen pr. e-mail og telefon uden unødig forsinkelse og om muligt senest 24 timer efter at være blevet bekendt med bruddet. Underretningen indeholder, i det omfang det er kendt: hvad der er sket og hvornår, hvilke kategorier og det omtrentlige antal registrerede og registreringer der er berørt, de sandsynlige konsekvenser, de foranstaltninger der er truffet eller foreslås, samt kontaktoplysninger hos databehandleren. Oplysninger, der ikke kendes ved første underretning, eftersendes løbende. Databehandleren stiller relevante logoplysninger til rådighed, fx loggen over visning og gemning af oplysninger i den separate database, og bistår efter anmodning med at formulere en underretning til de registrerede.

Konsekvensanalyse og forudgående høring (Bestemmelse 9.2.c–d): Databehandleren stiller efter anmodning en beskrivelse af systemet, dataflowet, underdatabehandlerne, sikkerhedsforanstaltningerne og de kendte begrænsninger til rådighed (bl.a. dokumentet "NGO Basen – Datasikkerhed" og disse Bestemmelser), besvarer den dataansvarliges spørgsmål til brug for konsekvensanalysen og bistår i nødvendigt omfang ved en forudgående høring af Datatilsynet.

C.4 Opbevaringsperiode/sletterutine

Personoplysninger opbevares, så længe den dataansvarlige anvender systemet, og indtil den dataansvarlige sletter dem via systemets funktioner. Den dataansvarlige fastsætter selv slettefrister for sine data og kan tildele slettefrister på enkelte personer i systemet. Ved ophør af tjenesten udleverer databehandleren efter anmodning oplysningerne i et almindeligt læsbart format og sletter dem derefter senest 30 dage efter ophøret, også i den separate database, i overensstemmelse med Bestemmelse 11.1, medmindre den dataansvarlige efter underskriften af disse Bestemmelser har ændret sit oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til Bestemmelserne. Når oplysninger er slettet, forsvinder de fra sikkerhedskopierne ved rotation: for den almindelige database senest ca. 14 dage efter sletningen og for den separate database senest 7 dage efter sletningen. Sikkerhedskopier kan ikke slettes enkeltvis. Lovable gemmer på Business-abonnementet som standard ikke det fulde indhold af AI-kald, kun et resumé af kaldet.

Opbevaring af logs hos underdatabehandlerne: Mailgun gemmer logs i op til 30 dage alt efter abonnement, og OpenAI gemmer API-data i op til 30 dage til misbrugsovervågning.

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:

Almindelig database og filer: Frankfurt, Tyskland (EU) – Lovable Cloud. Separat database til CPR-numre og følsomme oplysninger (pengeskabet): London, Storbritannien – Supabase Pte.

Ltd. Applikation og netværk: Cloudflares globale netværk (data i transit). Afsendelse af e-mails og AI-hjælp ved import: USA – via Lovable, jf. Bilag B. Databehandlerens support og drift: Danmark.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Storbritannien: Den separate database (pengeskabet) ligger i London. Overførslen sker på grundlag af EU-Kommissionens afgørelse om tilstrækkeligt beskyttelsesniveau for Storbritannien, jf. databeskyttelsesforordningens artikel 45 (afgørelse (EU) 2021/1772, fornyet ved afgørelse (EU) 2025/2574 og gældende til 27. december 2031). Supabase Pte. Ltd. er hjemmehørende i Singapore; eventuel adgang fra lande uden for EU/EØS og Storbritannien, fx ved support, er omfattet af EU-Kommissionens standardkontraktbestemmelser (afgørelse (EU) 2021/914) i Supabases databehandleraftale.
USA: Cloudflare (data i transit), Mailgun (e-mails) og OpenAI (AI-hjælp ved import) anvendes via Lovable. Lovable Labs Incorporated er selv hjemmehørende i USA. Overførslerne er omfattet af databehandleraftalen med Lovable, hvorefter overførsler uden for EU/EØS sker på grundlag af EU-Kommissionens standardkontraktbestemmelser (afgørelse (EU) 2021/914), som indgår i aftalen, eller et andet gyldigt overførselsgrundlag efter databeskyttelsesforordningens kapitel V. Øvrige oplysninger opbevares i EU. Databehandleren flytter ikke oplysninger til andre lande uden den dataansvarliges forudgående skriftlige godkendelse. Overførslerne bygger på standardkontraktbestemmelserne og ikke alene på EU-USA-databeskyttelsesrammen (Data Privacy Framework), da afgørelsen om rammen er indbragt for EU-Domstolen (sag C-703/25 P). Til AI-tjenesten sendes alene de oplysninger, der er beskrevet i Bilag C.1; CPR-numre, journalnotater og andre oplysninger fra den separate database sendes aldrig.

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

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren
Den dataansvarlige eller en repræsentant for den dataansvarlige kan én gang årligt samt ved en konkret mistanke om brud foretage inspektion af de systemer og procedurer, databehandleren anvender til behandlingen, med henblik på at fastslå databehandlerens overholdelse af databeskyttelsesforordningen og disse Bestemmelser. Inspektionen kan ske gennem dokumentation, dialog og teknisk gennemgang. Den dataansvarliges eventuelle udgifter i forbindelse med inspektionen afholdes af den dataansvarlige selv. Databehandleren er forpligtet til at afsætte de ressourcer, der er nødvendige for, at den dataansvarlige kan gennemføre sin inspektion.

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere
Databehandleren kontrollerer løbende, at underdatabehandlerne overholder deres databehandlerforpligtelser, herunder gennem gennemgang af underdatabehandlernes sikkerhedsdokumentation og certificeringer. Dokumentation herfor stilles efter anmodning til rådighed for den dataansvarlige.

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

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

Bilag D Parternes regulering af andre forhold

1. Aftalegrundlag: Bestemmelserne supplerer NGO Basens handelsbetingelser. Ved uoverensstemmelse har Bestemmelserne forrang for så vidt angår behandling af personoplysninger.
2. Vederlag: Databehandlerens bistand efter Bestemmelse 9 og Bilag C.3, som ikke kan håndteres via systemets egne funktioner, er inkluderet i abonnementet i rimeligt omfang. Omfattende bistand, der skyldes den dataansvarliges forhold, kan faktureres efter forudgående aftale.
3. Ansvar: Parternes ansvar reguleres af dansk rets almindelige regler og NGO Basens handelsbetingelser, dog således at ingen begrænsning gælder i det omfang, den strider mod databeskyttelsesforordningen eller de registreredes rettigheder.
4. Den dataansvarliges egne integrationer: Den dataansvarlige er selv ansvarlig for sine aftaler med egen betalingsudbyder (fx Stripe) og med de systemer, der importeres data fra (fx Donorfy, OnlineFundraising, Viggo og Mailchimp).