CHANGELOG

VERSION	ÆNDRINGER
1.0.0	Første udgave
1.0.1	Teknisk rettelse i Bilag E
1.0.2	21-05-2024: Præcisering mht. underdatabehandlere og opdeling af de registrerede, samt tilføjelse af dataflow bilag F
1.0.3	21-06-2024: Rettelser i instruktion til leverandøren, Præcisering af bilag A og bilag C
1.0.4	15-08-2024: præciseringer og rettelser i afsnit 14, 15 C.4, C.7 og C.8
1.0.5	15-11-2024: rettelser og præciseringer i afsnit B.1 (Underdatabehandlere), C.2, afsnit 10 (Hjemme- og fjernarbejdspladser) og C.5 (Lokationer for behandling)
1.0.6	Renset for kommentarer og tidligere track changes godkendt. Snip af koncerndiagram indsat i Bilag D.
1.0.7	Præcisering omkring i C.5 omkring ansvar for anonymisering samt omfang af kryptering og opbevaring af krypteringsnøgle. Opdatering af organisationsdiagrammer vedrørende underdatabehandlere i bilag E.

Databehandleraftale

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

mellem
Aarhus Kommune
CVR 55133018
Rådhuspladsen 28000 Aarhus C
Danmark
herefter "den dataansvarlige"

og

Deloitte Statsautoriseret Revisionspartnerselskab
CVR 33963556
Weidekampsgade 6
2300 København S
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

Indholdsfortegnelse

1. Præambel 4
2. Den dataansvarliges rettigheder og forpligtelser 5
3. Databehandleren handler efter instruks 5
4. Fortrolighed 5
5. 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 12
Bilag A Oplysninger om behandlingen 13
Bilag B Underdatabehandlere 16
Bilag C Instruks vedrørende behandling af personoplysninger 18
Bilag D Parternes regulering af andre forhold 27
Bilag E Databehandlerkæden 29
Bilag F Dataflowdiagram 30

1. 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 Chat- og Voicebot 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 seks 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. Bilag E indeholder en beskrivelse af databehandlerkæden

11. Bilag F indeholder et dataflowdiagram

12. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

13. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

2. 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.

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.

3. 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.

4. 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.

5. 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,

1 Henvisninger til "medlemsstat" i disse bestemmelser skal forstås som en henvisning til "EØS-medlemsstater".

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:

i. pseudonymisering og kryptering af personoplysninger

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

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

iv. 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 ved- kommende 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 plan- lagte 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 databeskyttelses- forordningen.

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

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

6. Databehandleren skal i sin aftale med underdatabehandleren, hvis muligt, indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

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

8. Overførsel til tredjelande eller internationale organisationer

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

2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal

databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

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

    i. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
    ii. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
    iii. 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:

    i. oplysningspligten ved indsamling af personoplysninger hos den registrerede
    ii. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
    iii. indsigtsretten
    iv. retten til berigtigelse
    v. retten til sletning (”retten til at blive glemt”)
    vi. retten til begrænsning af behandling
    vii. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
    viii. retten til dataportabilitet
    ix. retten til indsigelse
    x. 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:

i. 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

ii. 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

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

iv. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Data- tilsynet, 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:

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

ii. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

iii. 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, 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 skriftligt varsel af begge parter.

5. Underskrift

På vegne af den dataansvarlige

Navn:	Lene Hartig Danielsen
Stilling:	Chef for Borgerservice, Aarhus kommune
Telefonnummer:	+45 2920 4355
E-mail:	lha@aarhus.dk

.....
Dato / Underskrift:

På vegne af databehandleren

Navn:	Michael Theill
Stilling:	Partner
Telefonnummer:	+45 2220 2361
E-mail:	mtheill@deloitte.dk

.....
Dato / 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.

   Kontaktperson hos den dataansvarlige:

Navn:	Torben Glock
Stilling:	Special Consultant, Project Manager
Telefonnummer:	+45 3069 0120
E-mail:	tgl@aarhus.dk

Kontakt hos den dataansvarlige ved sikkerhedsbrud jf. afsnit 10:

E-mail:	Databeskyttelse(DPO) Borgerservice@aarhus.dk tgl@aarhus.dk.

Kontaktperson hos databehandleren:

Navn:	Marianne Horsager
Stilling:	Senior Manager
Telefonnummer:	+45 3093 4321
E-mail:	mhorsager@deloitte.dk

Bilag A Oplysninger om behandlingen

Chatbot: Databehandleren skal behandle spørgsmål, som stilles af borgeren via en chat på DDH-medlemskommunens hjemmeside. Borgeren kan i princippet skrive hvad som helst i Chatbot-dialogen, som derfor potentielt kan indeholde alle former for personoplysninger. Der vil blive foretaget sletning af personhenførbare data så tidligt i dataprocessen som muligt. Se bilag F. Databehandleren vil via chatbotten levere et matchende svar tilbage til borgeren. Disse svar er foruddefinerede og kvalitetsgodkendt af systemets Administratorer. Den anonymiserede chatdialog vil blive gemt og brugt til at træne den regelbaserede chatbot. Dialogerne vil kun være tilgængelige for et meget begrænset antal Administratorer, som er kommunalt ansatte borgerservicemedarbejdere

Voicebot: Databehandleren skal behandle spørgsmål, som stilles af borgeren via en telefonisk dialog. Borge- ren kan i princippet sige hvad som helst i voicebot-dialogen, som derfor potentielt kan indeholde alle former for personoplysninger. Det indtalte bliver transskriberet og sendt til chatbotten som tekst. Lyd- filen med borgerens stemme slettes umiddelbart efter transskriberingen. Der vil blive foretaget sletning af personhenførbare data så tidligt i dataprocessen som muligt. Se bilag F. Databehandleren vil via chatbotten levere et matchende svar tilbage til borgeren. Disse svar er foruddefinerede og kvalitetsgodkendt af systemets Administratorer. Svaret vil blive omdannet til en lydfil, som vil blive afspillet for borgeren.

Livechat og telefonsupport: Chatbotten kan videreformidle et telefonnummer til DDH's callcenter for evt. vejledning af en callcenter Agent eller en chat Agent, hvis Chatbotten ikke kan svare fyldestgørende. I denne videreformidling kan chatdialogen medsendes. Efter afsluttet dialog med callcenteragenten slettes den medsendte chatdialog umiddelbart efter.

Brug af LLM: Chat/voicebotten kan benytte generativ AI (LLM) til at besvare spørgsmål, hvor det skønnes hensigtsmæssigt og forsvarligt. Den generative AI vil kun behandle anonymiserede dialoger. LLM trænes ikke på de anonymiserede dialoger.

Selvbetjeningsløsninger: Chat/voicebotten kan interagere med digitale selvbetjeningsløsninger via MitID og dermed hjælpe borgeren til at udfylde digitale formularer.

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

Formålet med behandlingen er at give Borgeren information og hjælp mht. generelle spørgsmål i forhold til kontakt til den Dataansvarlige og skal fungere som et supplement til den Dataansvarliges øvrige kommunikationskanaler såsom fysisk fremmøde, kontaktcenter, hjemmesider og sociale medier.

Formålet med behandlingen er at højne serviceniveauet ved at give borgeren konkrete, lovmedholdelige, kvalitetssikrede svar også udenfor den Dataansvarliges åbningstid.

Formålet er tillige at kunne tilbyde en alternativ brugergrænseflade til udfyldelse af kommunale selvbetjeningsløsninger

Behandlingen har ikke til formål at besvare spørgsmål på konkrete sager og afgørelser, ligesom behandlingen heller ikke har til formål at komme med eller understøtte afgørelser.

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

Behandlingen drejer sig alene om besvarelse af generelle spørgsmål relateret til den Dataansvarliges opgaver, samt hjælp til udfyldelse af digitale selvbetjeningsløsninger.

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

Bemærk bilag F – dataflowdiagrammet hvoraf fremgår at personoplysninger bliver i chatbotten anonymiseret umiddelbart efter modtagelse af borgers oplysninger og løbende i samtalen.
I voicebot bliver personoplysninger anonymiseret umiddelbart efter transskribering, og hverken lydfil eller transskribering gemmes.
De personoplysninger, som kun behandles kortvarigt (mindre end 5 sekunder) inden de anonymiseres, er markeret med blå.

REGISTREREDE / PERSON-OPLYSNINGER	Borgere, chatbot	Borgere, Voicebot	Ansatte
Almindelige person-oplysninger: (art. 6)	☒ Navn ☒ Adresse ☒ E-mail ☒ Telefonnummer ☒ Fødselsdato ☐ ☐ Billeder ☒ Andre almindelige personoplysninger: Vil-kårligt angivne oplysnin- ger fra borger	☒ Navn ☒ Adresse ☒ E-mail ☒ Telefonnummer ☒ Fødselsdato ☒ Stemme ☐ Billeder ☒ Andre almindelige personoplysninger: Vil-kårligt angivne oplysnin- ger fra borger	☒ Navn ☐ Adresse ☒ E-mail ☐ Telefonnummer ☐ Fødselsdato ☒ Medarbejder ID ☐ Billeder ☒ Andre almindelige personoplysninger: - Kommunetilhørsfor-hold - Loginoplysninger
Følsomme personoplysninger: (art. 9)	☒ Race eller etnisk op-rindelse ☒ Politisk, religiøs eller filosofisk overbevis- ning ☒ Fagforeningsmæs- sige tilhørsforhold ☐ Genetisk data ☐ Biometrisk data ☒ Helbredsoplysninger ☒ Seksuelle forhold el- ler orientering	☒ Race eller etnisk op-rindelse ☒ Politisk, religiøs eller filosofisk overbevis- ning ☒ Fagforeningsmæs- sige tilhørsforhold ☐ Genetisk data ☐ Biometrisk data ☒ Helbredsoplysninger ☒ Seksuelle forhold el- ler orientering	☐ Race eller etnisk oprindelse ☐ Politisk, religiøs eller filosofisk overbevisning ☐ Fagforeningsmæssig e tilhørsforhold ☐ Genetisk data ☐ Biometrisk data ☐ Helbredsoplysninger ☐ Seksuelle forhold el- ler orientering
Straffedomme og lovovertrædelser (§10)	☒ Straffedomme og lov-overtrædelser	☒ Straffedomme og lov-overtrædelser	☐ Straffedomme og lov-overtrædelser
CPR-nummer (§11)	☒ CPR-nummer	☒ CPR-nummer	☐ CPR-nummer
Andre fortrolige per-sonoplysninger	☒ Væsentlige sociale forhold ☒ Væsentlige økonomi-ske forhold	☒ Væsentlige sociale forhold ☒ Væsentlige økonomi-ske forhold	☐ Væsentlige sociale forhold ☐ Væsentlige økonomi-ske forhold

	☒ Bankoplysninger ☐ Ansøgninger og CV ☒ Andre fortrolige oplysninger: Vilkårligt angivne oplysninger fra borger	☒ Bankoplysninger ☐ Ansøgninger og CV ☒ Andre fortrolige oplysninger: Vilkårligt angivne oplysninger fra borger	☐ Bankoplysninger ☐ Ansøgninger og CV ☐ Andre fortrolige oplysninger: [beskriv hvilke]

A.4. Behandlingen omfatter følgende kategorier af registrerede

Se A.3

Der vil være tre kategorier af registrerede:

- Borgere, som benytter chatbotten til skriftlig dialog.
- Borgere, som benytter voicebotten til mundtlig dialog
- Medarbejdere, som arbejder med chatbotten.

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

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af parterne.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere, som er angivet ud i yderste led i databehandlerkæden:

NAVN	CVR/ VIRKSOMHEDS ID	ADRESSE OG LAND	BESKRIVELSE AF BEHANDLING
Boost AI AS	917362394	Grenseveien 21, 4313 Sandnes, Norge.	Leverance af chatbotløsning. Administration, support, teknisk støtte/udvikling.
Boost Ai Aps	42476854	Amager Strandvej 390-392 - 2770 Kastrup, Danmark.	Administration og support.
BT AI UK Ltd	13590473	87A Worship Street, Shoreditch, London, EC2A 2BE, UK	Administration og support.
BT AI Sweden AB	559283-7016	Epicenter, Malmskillnadsgatan 44A, 111 57 Stockholm, Sverige.	Administration og support.
Boost.ai Oy	FI32286453	c/o Sofia Helsinki members, Sofiankatu 4 C, 00170 Helsinki, Finland.	Administration og support.
Microsoft Ireland Operations, Ltd		One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521, Irland	i) Hosting, storage og backup af anonymiseret tekstdata fra boost.ais platform, ii) lydtransskribering af tale til tekst, samt tekst til tale, og iii) LLM på anonymiseret data. iiii) StT databehandling foregår in motion og gemmes ikke.
Amazon Web Services, EMEA SARL		8 Avenue, John F. Kennedy, L-1855, Luxembourg	Hosting, storage og backup af anonymiseret tekstdata.
VIER GmbH	DE301500566	Hamburger Allee 23 30161 Hannover, Tyskland	Viderestilling af taledata, samt forbindelse til telefonsystemer.
CANCOM GmbH Messerschmittstr. 20, 89343 Jettingen-Scheppach	DE87910364	Tyskland	Fjernvedligeholdelse af hardware og support i de datacentre, der bruges af VIER.

Germany			

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden at følge den aftalte procedure for udskiftning af underdatabehandlere – 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 indsigelse ved skift af underdatabehandlere

Se punkt 7.3 i Bestemmelserne.

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:

Den Dataansvarlige instruerer hermed Databehandleren om at foretage behandling af Kommunens oplysninger til brug for drift af ydelser jf. Hovedaftale af den 1. oktober 2024 *"Kontrakt om levering af it- løsning til en Chat- og Voicebot"*.

Databehandleren må ikke anvende oplysningerne til andre formål. Oplysningerne må ikke behandles efter instruks fra andre end den Dataansvarlige

C.2. Behandlingssikkerhed
Sikkerhedsniveauet skal afspejle behandlingens omfang og karakter:

<u>Oplysninger om behandlingen:</u>

Behandlingen omfatter følgende antal registrerede:

☐ Under 1000 (1 point)
☐ 1000 - 10.000 (2 point)
☒ Over 10.000 (3 point)

Behandlingen omfatter behandling af følgende type personoplysninger:

☒ Almindelige personoplysninger, art. 6 (0 point)

☒ Særlige kategorier af personoplysninger / Følsomme personoplysninger, art. 9 (3 point)

☒ Andre beskyttelsesværdige / fortrolige personoplysninger, (F.eks. oplysninger om private forhold omfattet af straffelovens § 152, jf. forvaltningslovens § 27, personnumre, jf. databeskyttelseslovens § 11, samt oplysninger om strafbare forhold, jf. databeskyttelseslovens § 10) (2 point)

☐ Særlige behandlinger (F.eks. Overvågning, kortlægning af adfærd, profilering, automatiske behandlinger) (2 point)

<u>Sikkerhedsniveau:</u>
På baggrund af de ovenfor angivne oplysninger om behandlingen, og under hensyntagen til behandlingens karakter, omfang, sammenhæng og formål, samt risiciene af varierende sandsynlighed og al- vor for fysiske personers rettigheder og frihedsrettigheder etableres følgende sikkerhedsniveau:

Meget lav (1-2 point)	Lav (3-4 point)	Middel (5-6 point)	Høj (7-10 point)
☐	☐	☐	☒

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 understøtte den Dataansvarlige i dennes arbejde med at dokumentere de identificerede risici og hvordan risikoen er nedbragt til et acceptabelt niveau og gennemføre de foranstaltninger, der er nødvendige for at imødegå identificerede risici.

På baggrund af det etablerede sikkerhedsniveau implementeres procedurer for revisioner i overensstemmelse med punkt C.7 og C.8.

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

KRAV TIL ANONYMISERING AF PERSONOPLYSNINGER

Databehandleren sikrer at den Dataansvarlige har mulighed for at foretage anonymisering af person-data så tidligt i dataflowet som muligt og sikrer at anonymiseringen er uigenkaldelig.

KRAV TILKRYPTERING AF PERSONOPLYSNINGER

Databehandler foretager kryptering af persondata, hvor den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers grundlæggende rettigheder og frihedsrettigheder tilsiger det.

Der anvendes kryptering af personoplysninger ved enhver transmission via eksterne kommunikationsforbindelser. Databehandler skal navnlig sikre, at:

1. Passwords er krypteret
2. Der er formaliserede procedurer for gennemførsel af kryptering
3. Krypteringen er baseret på anerkendte og tidssvarende algoritmer og har en styrke, der svarer til person- datas følsomhed og mængde
4. Personoplysninger krypteres på alle miljøer
5. Data er anonymiseret af databehandler. Krypteringsnøglen, kodenøglen eller lignende opbevares tillige forsvarligt og adskilt fra alle personoplysninger

KRAV VEDRØRENDE EVNEN TIL AT SIKRE VEDVARENDE FORTROLIGHED, INTEGRITET, TILGÆNGELIG-HED OG ROBUSTHED AF BEHANDLINGSSYSTEMER OG –TJENESTER

1. Databehandler foretager løbende mitigerende foranstaltninger af teknisk og organisatorisk karakter, når dette viser sig påkrævet. F.eks. som følge af databehandlerens opdaterede risikovurdering, efter et brud på persondatasikkerheden, vejledning fra it-revisionen og i forbindelse med revisionserklæringers udvisende.

2. Databehandler udbedrer uden ugrundet ophold udeståender, konstateret i forbindelse med udfærdigelse af revisionserklæringer

KRAV VEDRØRENDE PROCEDURER FOR REGELMÆSSIG AFPRØVNING, VURDERING OG EVALUERING AF EFFEKTIVITETEN AF DE TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER TIL SIKRING AF BEHANDLINGSSIKKERHEDEN

Databehandler har til enhver tid tidssvarende procedurer for gennemførelse af:

1. Regelmæssig kontrol, vurdering, tilpasning og forbedring af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Databehandler er underlagt efter den til enhver tid gældende lovgivning, retspraksis, Datatilsynets afgørelser, anbefalinger og retningslinjer samt vil- kårene i nærværende databehandleraftale.

2. Kontrol af, at sikkerhedsforanstaltningerne faktisk efterleves i forhold til den til enhver tid værende risiko for de registreredes rettigheder og frihedsrettigheder. Herunder bl.a. opdateret og korrekt:
    a. Brugeradgang
    b. Backup
    c. Kryptering
    d. Sikkerhedslogning
3. Kontrol af at kryptering faktisk sker, at krypteringsnøglen opbevares sikkert og adskilt fra alle personoplysninger

KRAV VEDRØRENDE BESKYTTELSE AF OPLYSNINGER UNDER TRANSMISSION

Data er krypteret i forbindelse med overførsel af data. Krypteringen følger den til enhver tid værende best practice for kryptering og holdes således løbende opdateret med valg af kommunikationsprotokoller, krypteringsalgoritmer og nøglelængder, for at sikre at krypteringen ikke har kendte sårbarheder. Fortiden er minimumsstandarden TLS version 1.2. tvungen.

KRAV VEDRØRENDE BESKYTTELSE AF OPLYSNINGER UNDER OPBEVARING

Data er krypteret når de opbevares på medier, herunder diske, sql servere etc. Krypteringen følger den til enhver tid værende best practice for kryptering og holdes således løbende opdateret med valg af krypteringsalgoritmer og nøglelængder således, at krypteringen ikke har kendte sårbarheder. For tiden er minimumsstandarden AES, med en minimumsnøglelængde på 192 bit.

KRAV VEDRØRENDE FYSISK SIKRING AF LOKALITETER, HVOR DER BEHANDLES OPLYSNINGER

Databehandler sikrer, at:

1. Der er passende sikkerhedsforanstaltninger mod enhver uautoriseret adgang til lokationer, hvor den Dataansvarliges data behandles. Databehandleren skal desuden, regelmæssigt, evaluere og forbedre effektiviteten af sådanne forhåndsregler
2. Behandlingen foregår fra lokationer, som er beskyttet mod skader forårsaget af fysiske forhold som f.eks., - men ikke begrænset til - brand, overophedning, vandskade, forsyningssvigt, tyveri eller hærværk.

KRAV VEDRØRENDE ANVENDELSE AF HJEMME-/FJERNARBEJDSPLADSER

Såfremt Databehandlerens ansatte som led i leveringen af de aftalte ydelser, behandler personoplysninger på deres bopælsadresse sker det under hensyn til mindst samme sikkerhedsniveau som på arbejdspladsen. Herunder brug af VPN -forbindelse og krypteret adgang ved opkobling til nettet. De ansatte modtager i øvrigt regelmæssig træning i informationssikkerhed. Databehandleren er ISO 27001 certificeret, hvilket således er standarden for Databehandlerens informationssikkerhed.

Databehandlerens medarbejdere er instrueret, i at der gælder de samme krav til behandling og håndtering af persondata og andre fortrolige oplysninger, som der gælder på databehandlerens lokationer. Dog er medarbejdere, der arbejder hjemme logget på arbejdspladsens it-systemer via VPN.

KRAV VEDRØRENDE LOGNING
Alle adgange til operationelle systemer er logget, og auditeret. Se Bilag 4: Løsningsbeskrivelsen

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:

Databehandleren vederlægges for bistand til den dataansvarlige i overensstemmelse med Hovedaftalen.

<u>Underretning af den dataansvarlige om anmodninger fra de registrerede</u>
Databehandleren skal uden unødig forsinkelse, efter at være blevet opmærksom herpå, skriftligt underrette den dataansvarlige om enhver anmodning rettet til databehandleren eller dennes underdatabehandlere fra en registreret om udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret. Databehandleren er ikke berettiget til at besvare anmodninger fra en registreret vedrørende udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret. Databehandleren skal på anmodning fra den dataansvarlige hjælpe med at opfylde den dataansvarliges forpligtelser i forhold til de registreredes rettigheder i henhold til gældende databeskyttelsesret.

<u>Bistand ved sikkerhedsbrud, herunder underretning af den dataansvarlige om sikkerhedsbrud</u>
Databehandlerens bistand i forbindelse med den dataansvarliges forpligtelser efter databeskyttelses-forordningens artikel 33 og 34 sker ved, at databehandleren indgiver de oplysninger, der følger af Bestemmelse 10.3, til den dataansvarlige inden for den frist, der følger af Bestemmelse 10.2. Databehandleren skal efterfølgende bistå den dataansvarlige ved på den dataansvarliges anmodning at stille de oplysninger til rådighed, som er nødvendige for, at den dataansvarlige kan foretage anmeldelse af brud på persondatasikkerheden til den kompetente tilsynsmyndighed eller som er nødvendige for, at den dataansvarlige kan underrette den registrerede herom.

<u>Bistand i forbindelse med risikovurderinger og konsekvensanalyser</u>
Databehandleren skal bistå den dataansvarlige ved at stille de nødvendige oplysninger til rådighed, så den dataansvarlige kan gennemføre de nødvendige risikovurderinger. Såfremt den dataansvarlige vurderer, at behandlingen sandsynligvis vil indebære en høj risiko for de registreredes rettigheder og frihedsrettigheder, skal databehandleren på anmodning fra den dataansvarlige bistå den dataansvar-lige i forbindelse med dennes forpligtelser efter databeskyttelsesforordningens artikel 35 og 36 ved at indgive de oplysninger til den dataansvarlige, der er nødvendige for, at den dataansvarlige kan foretage en konsekvensanalyse i overensstemmelse med artikel 35 og foretage en forudgående høring af den kompetente tilsynsmyndighed i overensstemmelse med artikel 36.

Sikring af tekniske og organisatoriske foranstaltninger
Databehandleren skal endelig sikre, at dennes tekniske og organisatoriske foranstaltninger gør det muligt for den dataansvarlige at overholde sine forpligtelser efter databeskyttelsesforordningens artikel 33-36, herunder f.eks. gennem de foranstaltninger vedrørende styring af sikkerhedsbrud, styring af aktiver, logning mv., der følger af bilag C.

C.4 Opbevaringsperiode/sletterutine
Personoplysningerne opbevares hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret.

Ved ophør af tjenesten eller disse Bestemmelser vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarliges oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

Det er aftalt, at der skal ske løbende sletning af samtlige samtaler, som er ældre end 90 dage dog således at den Dataansvarlige selv er ansvarlig for at opsætte de nødvendige indstillinger i løsningen i relation til omfang og frekvens af den løbende sletning af personoplysninger.

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:

Virksomhedens navn og adresse	CVR eller andet virk-somheds ID	Lokalitet for behandling	Eventuelt overførselsgrundlag
Boost AI AS, Grenseveien 21, 4313 Sandnes	917362394	Norge	N/A
Boost Ai Aps Amager Strandvej 390-392 - 2770 Kastrup	42476854	Danmark	N/A
BT AI Sweden AB, Epicenter, Malmskillnadsgatan 44A, 111 57 Stockholm, Sverige.	559283-7016	Sverige	N/A
Boost.ai Oy, c/o Sofia Helsinki members, Sofiankatu 4 C, 00170 Helsinki, Finland.	FI32286453	Finland	N/A
BT AI UK Ltd, 87A Worship Street, Shoreditch, London, EC2A 2BE, UK	13590473	UK	Tilstrækkelighedsafgørelse udstedt af EU-Kommissionen.
Microsoft Ireland Operations Ltd		Sverige og/eller Region West-EU.	Microsoft er certificeret under EU-US Data Privacy Framework og i tillæg hertil EU Standard Contractual Clauses. Det er den Dataansvarliges ansvar at

			anonymiseringsfunktionen er aktiveret som aftalt. Data er krypteret og Databehandler har ikke adgang til krypteringsnøglen.
Amazon Web Services, EMEA SARL 8 avenue John F. Kennedy, L-1855 Luxembourg	921 416 873 MVA	Irland, backup i Tyskland	Amazon er certificeret under EU-US Data Privacy Framework og i tillæg hertil EU Standard Contractual Clauses. Det er den Dataansvarliges ansvar at anonymiseringsfunktionen er aktiveret som aftalt.
VIER GmbH Hamburger Allee 23 30161 Hannover, Tyskland	DE301500566	Tyskland	N/A
CANCOM GmbH Messerschmittstr. 20, 89343 Jettingen-Scheppach Germany	DE87910364	Tyskland	N/A

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Instruks og garanti, såfremt der ikke må ske overførsel og behandling udenfor EU/EØS
Databehandleren må ikke indenfor rammerne af disse Bestemmelser overføre personoplysninger til et land udenfor EU/EØS.

Alle data, herunder personoplysninger, behandles og opbevares indenfor EU, og må ikke direkte eller indirekte helt eller delvist tilgås fra lande udenfor EU/EØS. Se yderligere i Bilag 4: Løsningsbeskrivelse

Databehandleren indestår for, at alle data, herunder personoplysninger, som Databehandleren via alle sine underdatabehandlere behandler på vegne af den Dataansvarlige i henhold til disse Bestemmelser ikke i nogen tilfælde, hverken af tekniske eller kommercielle grunde overføres til og behandles i tredjelande.

Databehandleren garanterer, at personoplysninger ikke overføres til tredjelande i forbindelse med brug af Databehandlerens tjeneste eller levering af Databehandlerens ydelser omfattet af denne Databehandleraftale eller underdatabehandlerens ydelser, uanset om sådan overførsel sker af tekniske eller kommercielle grunde.

På den Dataansvarliges anmodning skal Databehandleren udlevere dokumentation af såvel tjenestens overførelsesmuligheder samt de tekniske og procesmæssige foranstaltninger, som Databehandleren har fastsat for at undgå utilsigtede overførsler af personoplysninger til lande udenfor EU/EØS. Se Bilag E og F for så vidt angår Databehandlers koncerndiagrammer og teknisk mitigerende foranstaltninger.

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

Databehandleren skal én gang årligt for egen regning indhente en revisionserklæring fra en uafhængig tredjepart angående databehandlerens overholdelse af databeskyttelsesforordningen, data- beskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Revisionserklæringen skal være af typen ISAE 3000 GDPR type 2 med høj grad af sikkerhed udarbejdet efter partiel metoden, dækkende kravene beskrevet i denne databehandleraftale. Revisionserklæringen fremsendes til den dataansvarlige.

Den dataansvarlige kan fravige den aftalte tilsynsform, såfremt den dataansvarlige vurderer, at databehandleren på anden vis vil kunne dokumentere overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser med tilhørende bilag.

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

Den dataansvarlige, eller en uafhængig revisor bemyndiget af den dataansvarlige, har endvidere ret til at foretage inspektioner af databehandlerens fysiske faciliteter, hvor der behandles personoplysninger, og systemer, der anvendes og har relation til behandlingen, samt modtage de nødvendige in- formationer til udførelsen af undersøgelsen af, hvorvidt databehandleren har truffet de sikkerheds- foranstaltninger, der følger af disse Bestemmelser samt gældende databeskyttelsesret. Den dataansvarlige indhenter en erklæring om fortrolighed fra den uafhængige revisor.

Den dataansvarlige kan anfægte rammerne for de foretagne kontrolforanstaltninger og kan i sådanne tilfælde anmode om en (ny) revisionserklæring og/eller (ny) inspektion under andre rammer og/eller under anvendelse af anden metode.
Den dataansvarlige er berettiget til at videregive informationer modtaget i henhold til bestemmelserne i nærværende bilag til den kompetente tilsynsmyndighed efter anmodning herom fra myndig- heden.

Databehandleren skal årligt for egen regning afgive en erklæring angående databehandlerens og dennes eventuelle underdatabehandleres overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser med tilhørende bilag.

Såfremt den dataansvarlige vurderer, at den fremsendte erklæring ikke på tilstrækkelig vis godtgør databehandlerens og dennes eventuelle underdatabehandleres overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser med tilhørende bilag, skal databehandleren på den dataansvarliges anmodning og for databehandlerens regning fremsende den nødvendige dokumentation til påvisning af overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser med tilhørende bilag

Den dataansvarlige, eller en uafhængig revisor bemyndiget af den dataansvarlige, har endvidere ret til med rimeligt varsel at foretage inspektioner af Databehandlerens fysiske faciliteter, hvor der behandles personoplysninger, og systemer, der anvendes og har relation til behandlingen, samt mod- tage de nødvendige informationer til udførelsen af undersøgelsen af, hvorvidt databehandleren har truffet de sikkerhedsforanstaltninger, der følger af disse Bestemmelser samt gældende databeskyttelsesret. Det kan eksempelvis være tilfældet, hvis en konkret omstændighed, f.eks. et sikkerheds- brud, giver anledning til tvivl om beskyttelsen af personoplysningerne hos databehandleren. Den dataansvarlige indhenter en erklæring om fortrolighed fra den uafhængige revisor.

Den dataansvarlige kan anfægte rammerne for de foretagne kontrolforanstaltninger og anmode om supplerende dokumentation af databehandlerens og dennes eventuelle underdatabehandleres overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser med tilhørende bilag

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

Den dataansvarlige er berettiget til at videregive informationer modtaget i henhold til bestemmelserne i nærværende bilag til den kompetente tilsynsmyndighed efter anmodning herom fra myndigheden.

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

Databehandleren træffer valg om, hvordan revision af underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og underdatabehandleraftalen foretages, herunder hvilken type af revisionserklæring og/eller inspektionsrapport, der indhentes. Typen og omfanget af revisionen skal afspejle karakteren af den behandling af personoplysninger, som underdatabehandleren foretager. Revisionserklæringer og/eller inspektionsrapporter fra ansvarlig uafhængig 3. part fremsendes minimum 1 gang årligt til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde anmode om en ny revisionserklæring under andre rammer og/eller under anvendelse af anden metode.

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

Den dataansvarlige kan efter aftale med Databehandleren – hvis det findes nødvendigt og er muligt – vælge med rimeligt varsel 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.

Den dataansvarliges eventuelle udgifter i forbindelse med en inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion. Databehandlerens og underdatabehandlerens eventuelle udgifter i forbindelse med afholdelse af et fysisk tilsyn/en inspektion hos underdatabehandleren er den dataansvarlige uvedkommende – uanset at den dataansvarlige har initieret og eventuelt deltaget på et sådant tilsyn.

Den dataansvarlige er berettiget til at videregive informationer modtaget i henhold til bestemmelserne i nærværende bilag til Datatilsynet efter anmodning herom fra Datatilsynet.

Bilag D Parternes regulering af andre forhold

D.1 Databehandlerkæden
Databehandleren skal udarbejde en fuldstændig oversigt over Databehandlere, som behandler den dataansvarliges personoplysninger. Oversigten udarbejdes og vedlægges i Bilag E.

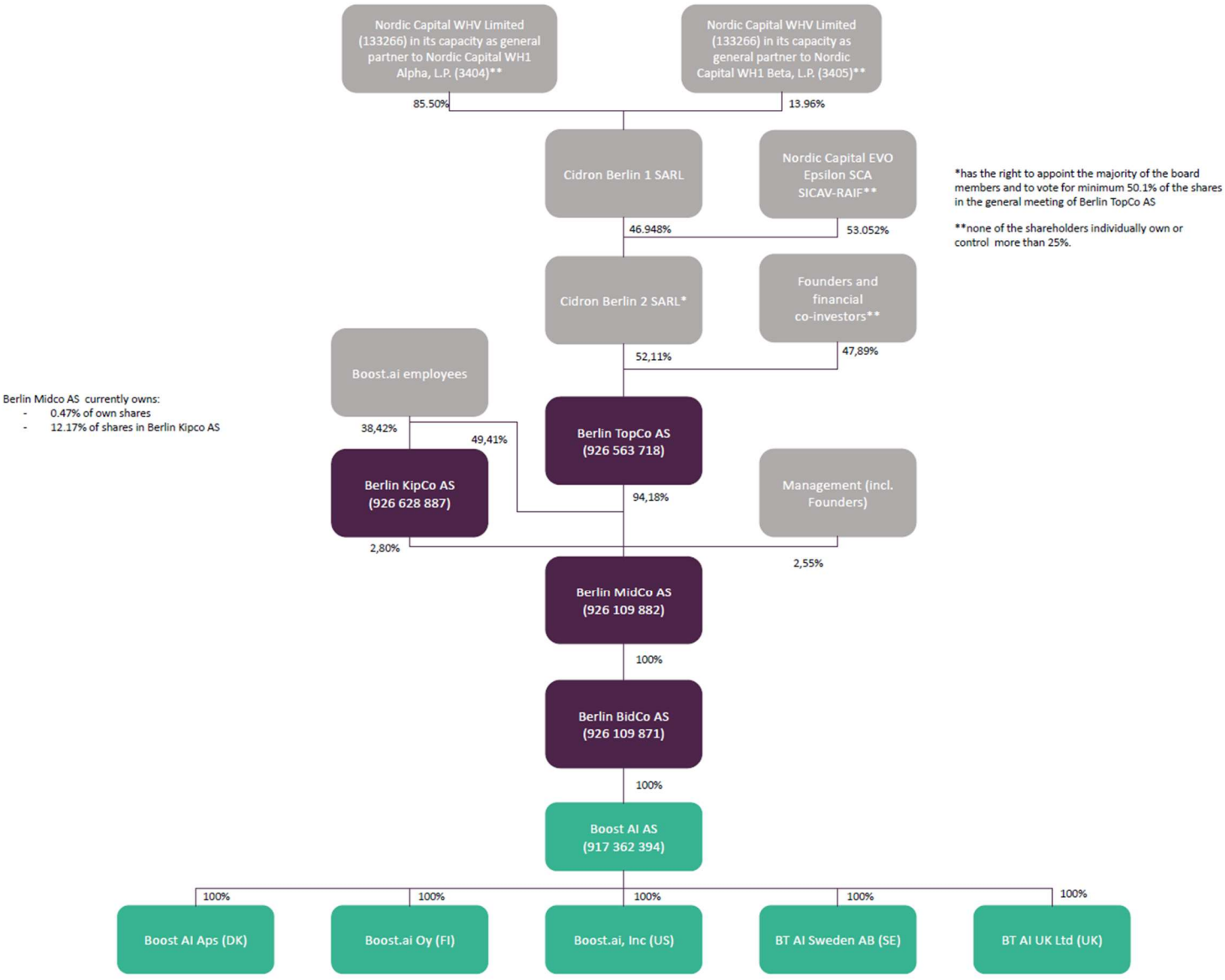
Oversigten skal angive databehandlerens underdatabehandlere, og alle deres eventuelle underdata-behandlere, så hele kæden for behandling af personoplysninger er dokumenteret.

Databehandleren orienterer den dataansvarlige om enhver ændring i databehandlerkæden og ændringer af ejerskab af selskaber i databehandlerkæden.

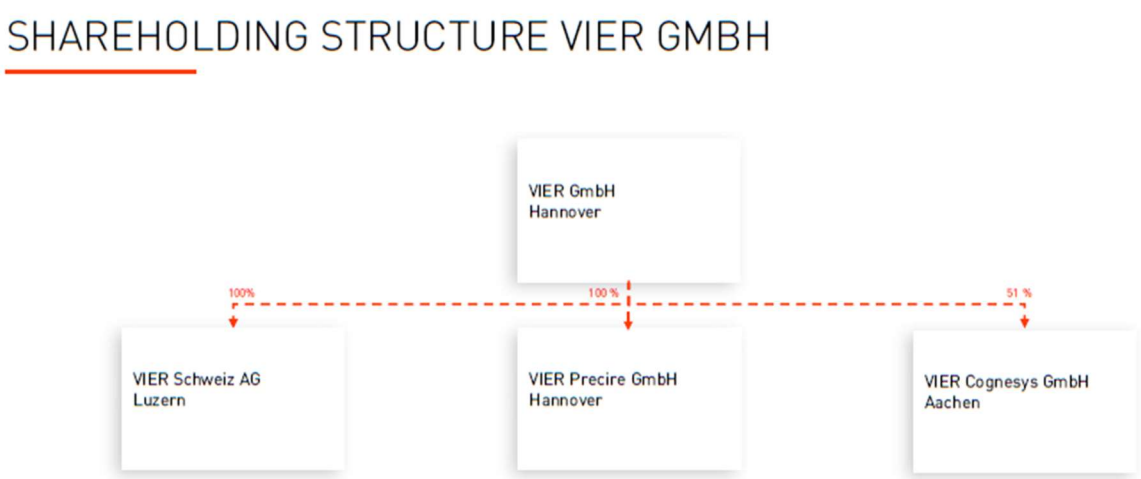
Databehandleren udarbejder et koncerndiagram over de koncernforbundne selskaber.
Databehandleren orienterer den dataansvarlige om enhver ændring af koncerndiagrammet.

Koncerndiagram for Boost AI AS

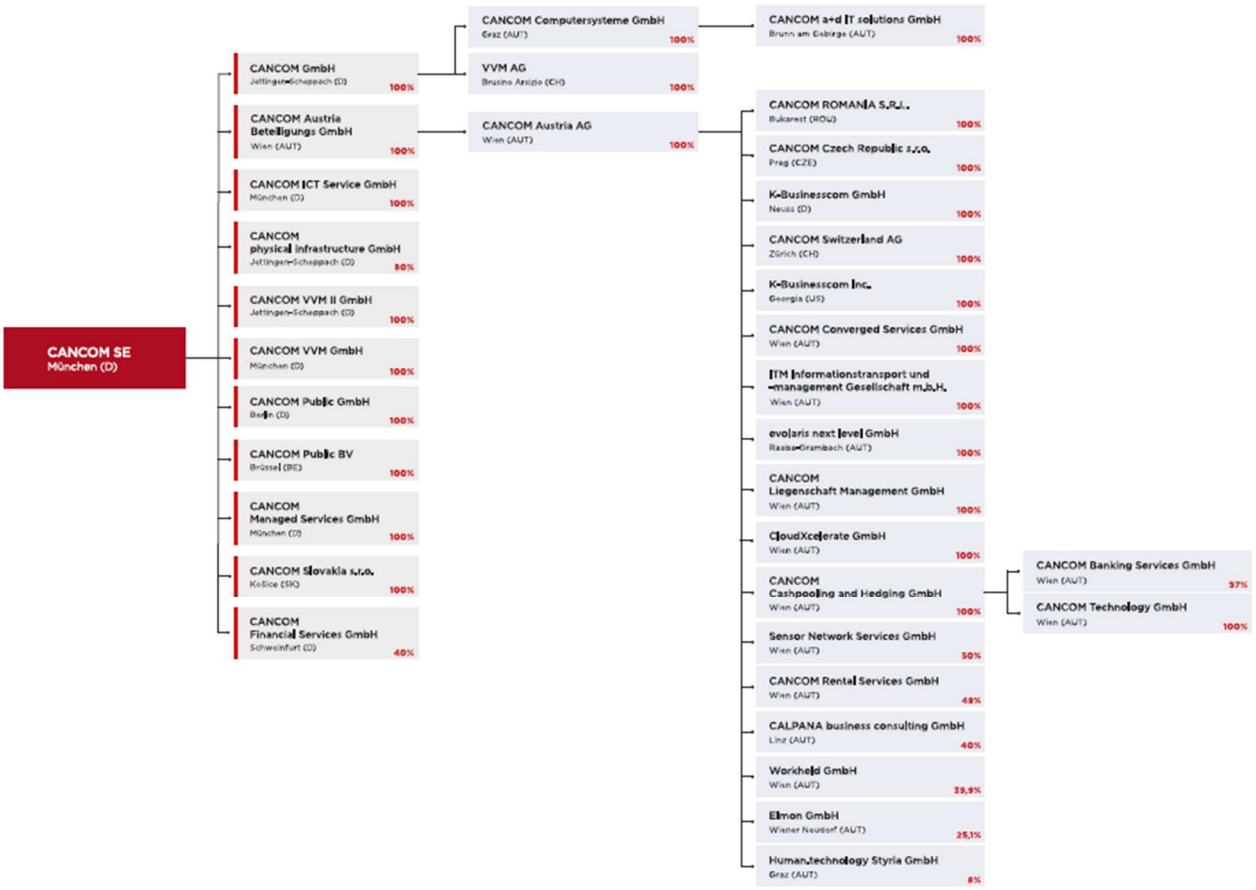
Udvalgte enheder markeret med turkis er involveret i databehandlingen, jf. Bilag E.



Koncerndiagram for Vier GmbH, Hannover



Koncerndiagram for CanCom GmbH, Jettingen-Scheppach



Bilag E Databehandlerkæden

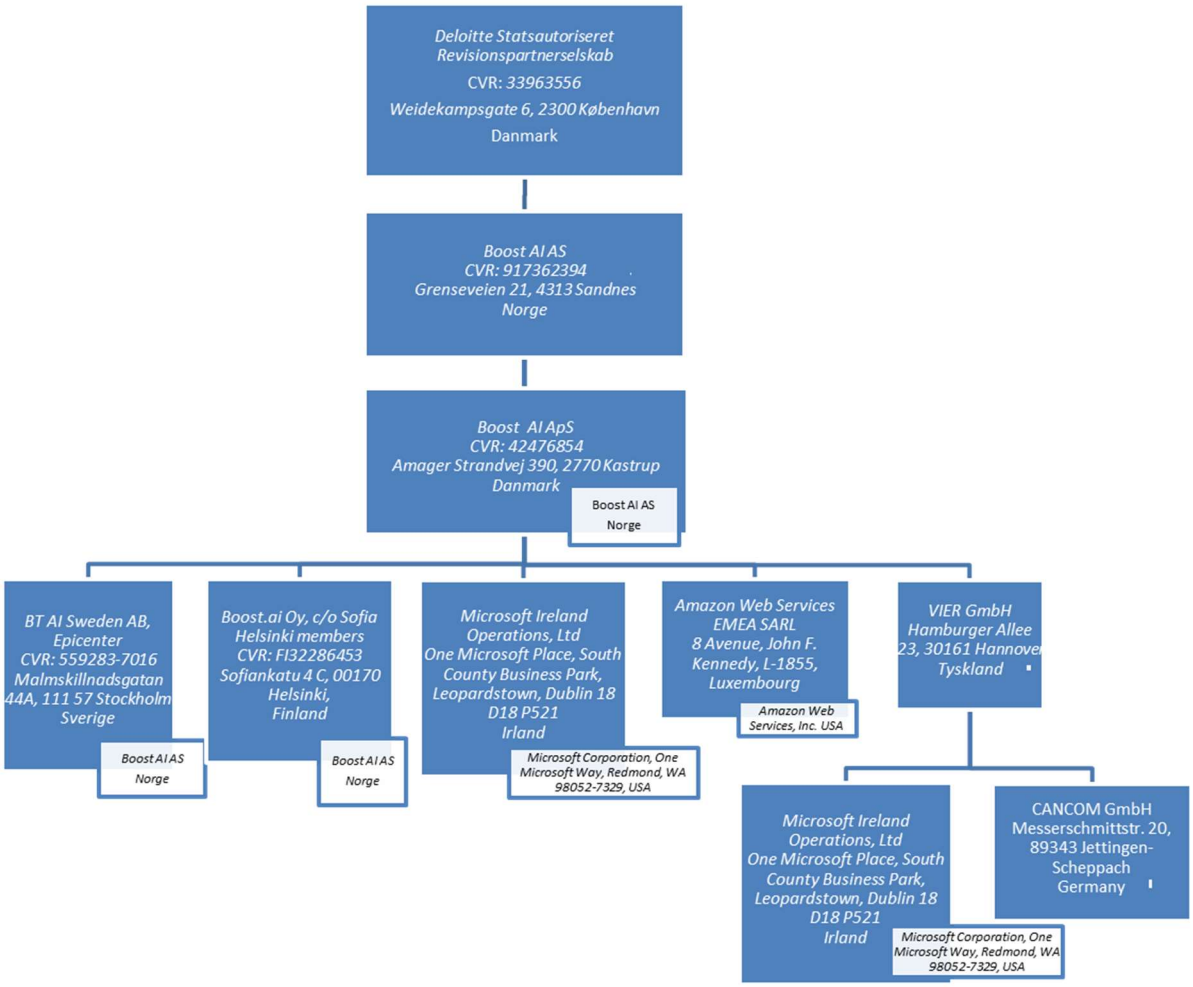
Oversigten viser en udtømmende liste over it-løsningens databehandlerkæde ud i yderste led.

Formålet er at dokumentere hvem, der behandler persondata for den dataansvarlige og hvor.

Målet er at have overblik over dataflowet og om der i kæden er Databehandlere, der er underlagt problematisk lovgivning eller praksis. Enten som følge af sin geografiske placering eller som følge af sin koncernforbindelse til et eller flere moderselskaber i ikke sikre tredjelande.

UDB er en forkortelse for UnderDataBehandler.
UUDB er en forkortelse for den pågældende underdatabehandlers UnderUnderDataBehandler etc.

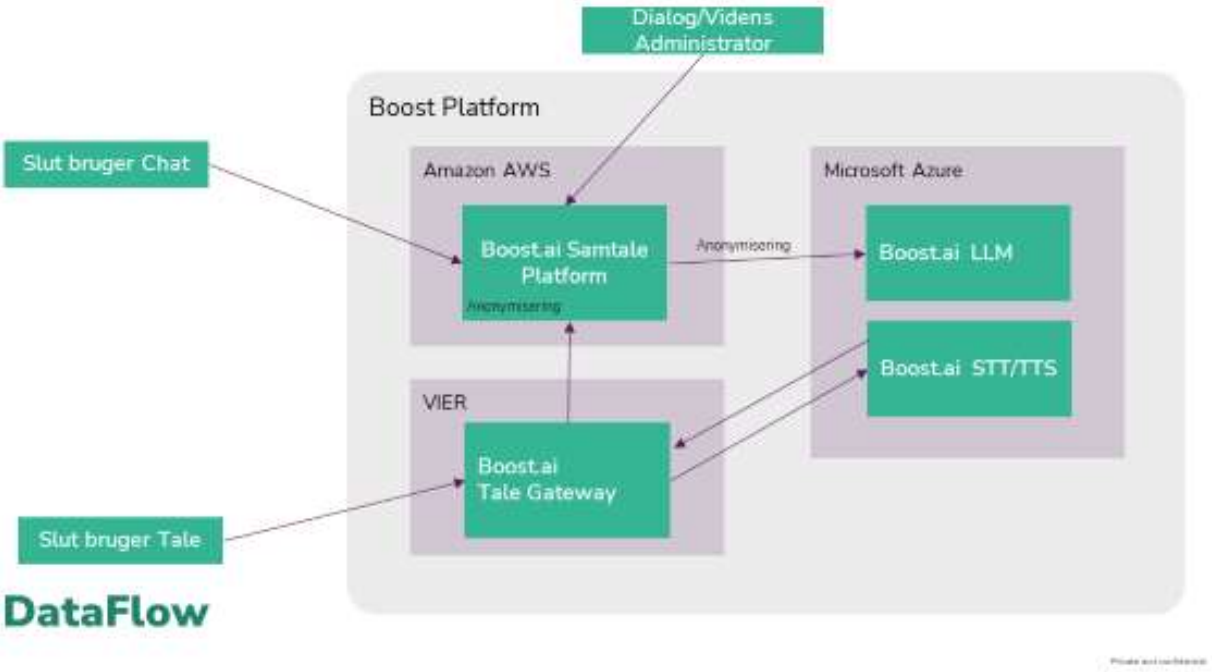
For hver databehandler angives korrekt firmanavn, id-nr. (i Danmark CVR-nr.), adresse og land. Databehandlers moderselskabs hjemsteds land angives nederst under hver databehandler.

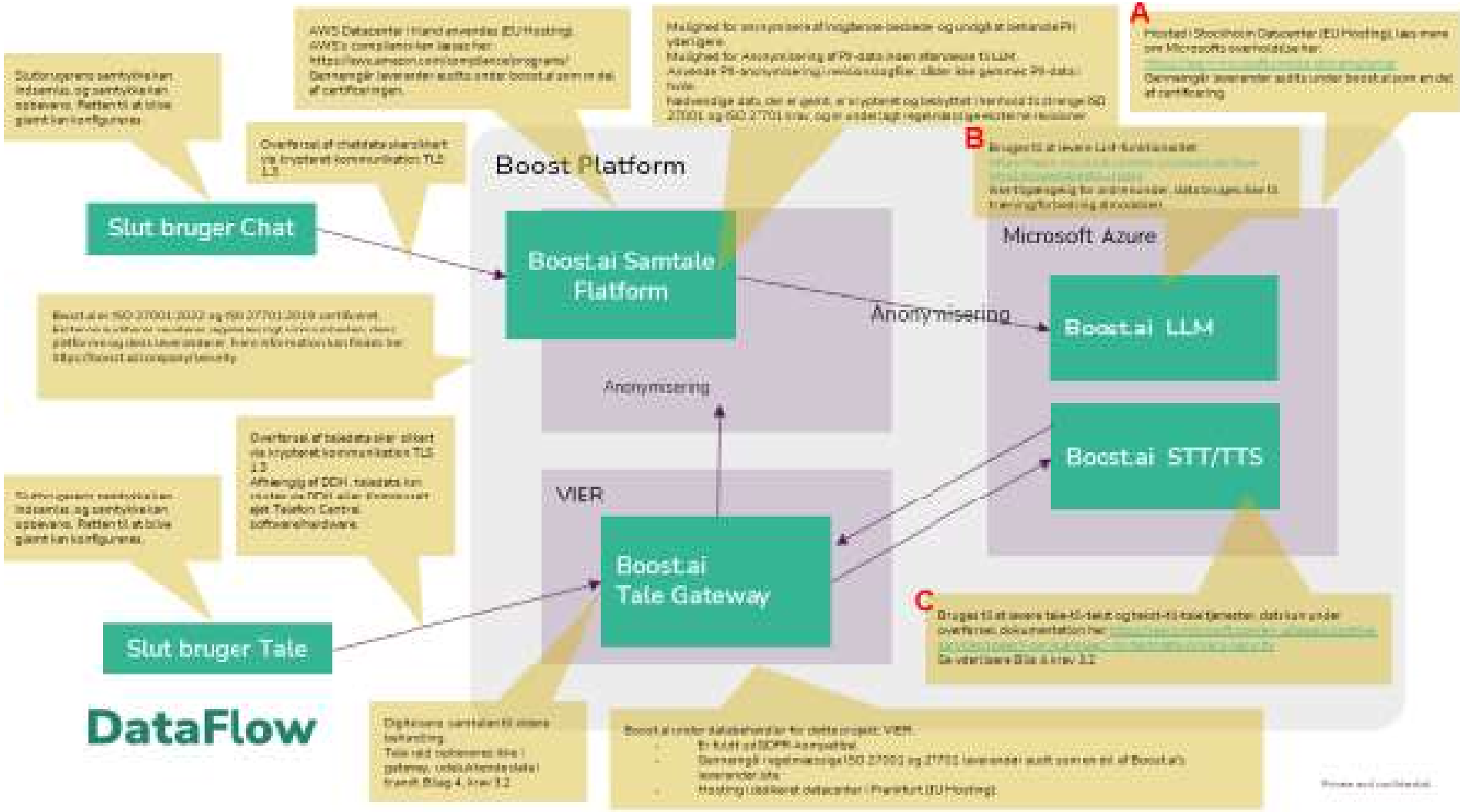


Bilag F Dataflowdiagram

Databehandleren skal udarbejde et udtømmende diagram over it-løsningens Dataflow fra start til slut. Både for Chatbot som for voicebot-delen. Hvis der sker anonymisering, bedes der angives hvor i flowet dette sker/kan ske.

Nedenstående Dataflow illustrerer hvor persondata behandles i de forskellige processer samt hvor i processen anonymisering finder sted.



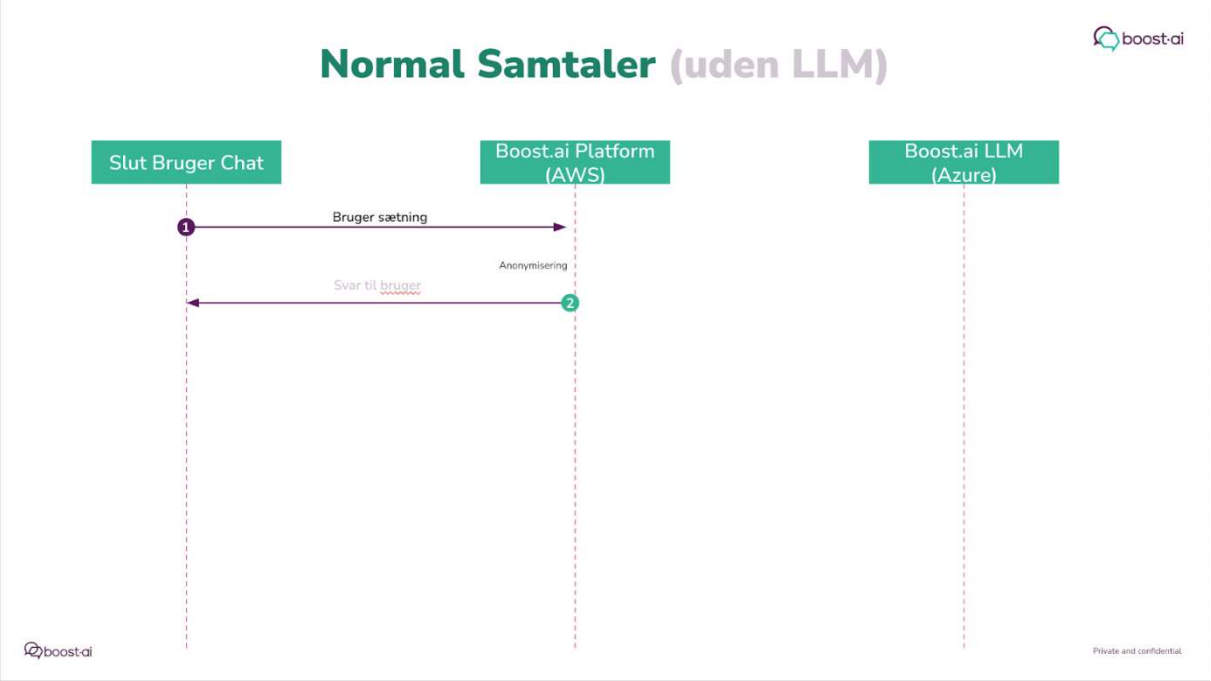

Slut bruger Chat
Slut bruger Tale
Boost Platform
Boost.ai Samtale Platform
Anonymisering
VIER
Boost.ai Tale Gateway
Microsoft Azure
Boost.ai LLM
Boost.ai STT/TTS
A
B
C
DataFlow

A- Hosted i Stockholm Datacenter (EU Hosting), læs mere om Microsofts overholdelse her:
https://learn.microsoft.com/da-dk/compliance/
Gennemgår leverandør audits under boost.ai som en del af certificering.

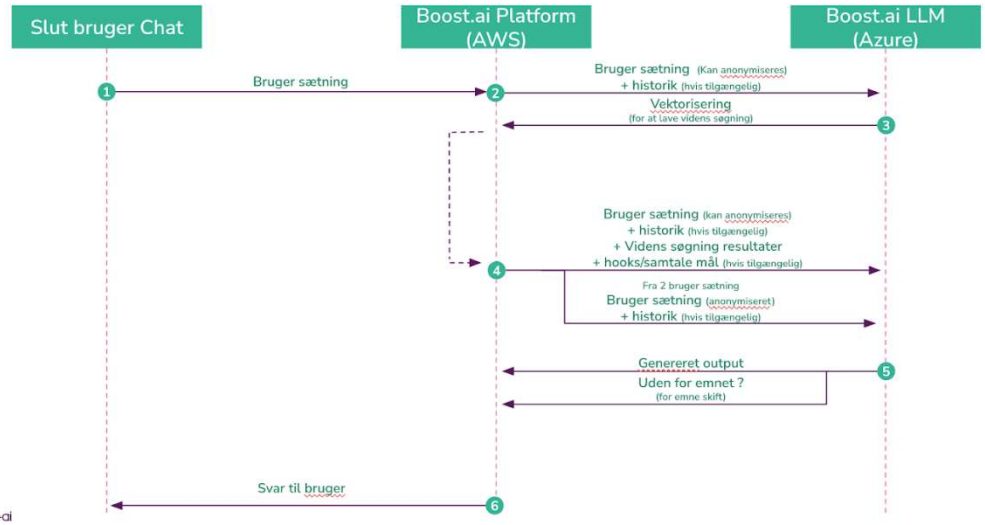
B- Bruges til at levere LLM-funktionalitet:
https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy
Ikke tilgængelig for andre kunder, data bruges ikke til træning/forbedring af modellen.

C- Bruges til at levere tale-til-tekst og tekst-til-tale tjenester, data kun under overførsel, dokumentation her:
https://learn.microsoft.com/en-us/legal/cognitive-services/speech-service/speech-to-text/data-privacy-security
Se yderligere Bilag 4, krav 3.2

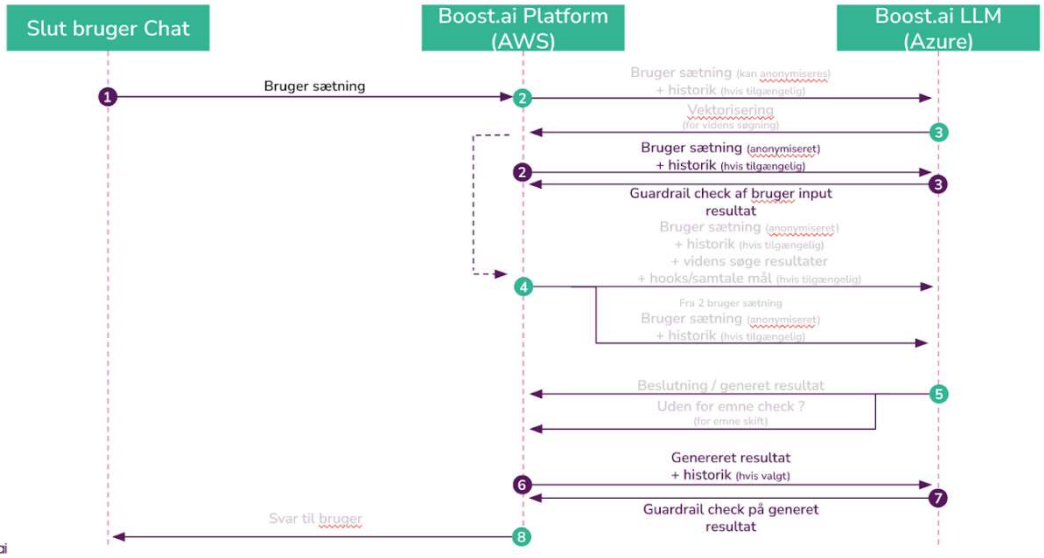
Microsoft levere STT/TTS service selv. Microsoft har ingen subprocessor leverandører i forbindelse med STT/TTS services. Den komplette liste af subprocessor for Microsoft er her:
https://servicetrust.microsoft.com/DocumentPage/e380d830-a35d-421b-971c-531ff90151e8
Ingen af disse leverandører er underdatabehandlere for TTS og STT servicen hos Microsoft.



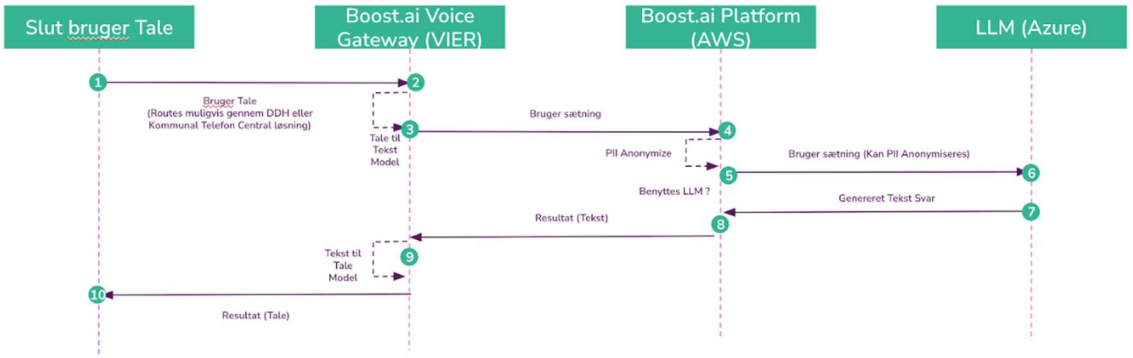
Generative Action: Grundlæggende



Generative Action: + Guardrails



Tale (Med eller uden LLM)



Generative Action: Tilføj viden