# Standardkontraktsbestemmelser

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

**Version 1.0 – 12. oktober 2026**

**mellem**

**Kunden**
Den virksomhed eller myndighed, der har oprettet en konto til Dansk LLM og accepteret disse Bestemmelser. Kundens juridiske navn, CVR-nummer og adresse fremgår af kontoen og af de fakturaer, Kunden modtager.

**herefter "den dataansvarlige"**

*og*

**Gavn Software ApS**
CVR 46177878
Ulrikkenborg Allé 23, 1. th.
2800 Kongens Lyngby
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.

Bestemmelserne følger Datatilsynets standardkontraktsbestemmelser (skabelon version 1.2). Afsnit 2–14 er Datatilsynets tekst med de valg, der er markeret i skabelonen. Det, der er særligt for Dansk LLM, står i bilag A–D.

# Indhold

2. Præambel
3. Den dataansvarliges rettigheder og forpligtelser
4. Databehandleren handler efter instruks
5. Fortrolighed
6. Behandlingssikkerhed
7. Anvendelse af underdatabehandlere
8. Overførsel til tredjelande eller internationale organisationer
9. Bistand til den dataansvarlige
10. Underretning om brud på persondatasikkerheden
11. Sletning og returnering af oplysninger
12. Revision, herunder inspektion
13. Parternes aftale om andre forhold
14. Ikrafttræden og ophør
15. Kontaktpersoner hos den dataansvarlige og databehandleren

Bilag A Oplysninger om behandlingen

Bilag B Underdatabehandlere

Bilag C Instruks vedrørende behandling af personoplysninger

Bilag D Parternes regulering af andre forhold

## 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 Dansk LLM (en sprogmodel, der stilles til rådighed via et API og en playground på platform.danskllm.dk) behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.
4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.
10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

## 3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller 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.

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

## 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.

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

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

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

## 8. Overførsel til tredjelande eller internationale organisationer

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

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

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

   a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation

   b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland

   c. behandle personoplysningerne i et tredjeland

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

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

## 9. Bistand til den dataansvarlige

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

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

   a. oplysningspligten ved indsamling af personoplysninger hos den registrerede

   b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede

   c. 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 dataansvarlige, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

## 12. Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.

2. 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 lovgivning har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

## 13. Parternes aftale om andre forhold

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 eller elektroniske accept 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. I stedet for fysisk underskrift kan parterne indgå Bestemmelserne elektronisk. Det sker ved, at den dataansvarlige ved oprettelsen af sin konto til Dansk LLM sætter flueben ved "Jeg accepterer vilkårene og privatlivspolitikken". Vilkårene for Dansk LLM henviser til disse Bestemmelser, som dermed er accepteret af den dataansvarlige. Databehandleren har accepteret Bestemmelserne ved at offentliggøre dem. Tidspunktet for accepten og den accepterede version gemmes på kontoen.

## 15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

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

**Hos databehandleren**

| | |
|---|---|
| Navn | Andreas Østerby Holst Rasmussen |
| Stilling | Direktør, Gavn Software ApS |
| Telefon | +45 41 82 11 62 |
| E-mail | info@gavn-software.dk |

**Hos den dataansvarlige**

| | |
|---|---|
| Navn og e-mail | Den e-mailadresse, kontoen er oprettet med, og den person, der har oprettet kontoen. Den dataansvarlige kan oplyse en anden kontaktperson ved at skrive til info@gavn-software.dk. |

# Bilag A Oplysninger om behandlingen

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

Formålet er at levere Dansk LLM til den dataansvarlige: en sprogmodel, som den dataansvarlige sender tekst til ("input") og får genereret tekst tilbage fra ("output"). Tjenesten tilgås via et API (api.danskllm.dk) fra den dataansvarliges egne systemer eller via playgrounden på platform.danskllm.dk.

Personoplysninger behandles kun, fordi og i det omfang den dataansvarlige selv lægger dem i sit input. Databehandleren bestemmer ikke, hvad input indeholder, og har ikke brug for personoplysninger for at levere tjenesten. Databehandleren anvender ikke input eller output til egne formål, herunder ikke til at træne eller forbedre sprogmodeller.

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

Behandlingen er en gennemløbsbehandling:

- Den dataansvarlige sender input over en krypteret forbindelse til databehandlerens gateway, som kontrollerer API-nøglen og saldoen og sender forespørgslen videre til en af databehandlerens egne GPU-servere.
- Sprogmodellen på GPU-serveren genererer output, som sendes tilbage til den dataansvarlige, mens det bliver til (streaming) eller samlet.
- Input og output gemmes ikke. De findes kun i serverens arbejdshukommelse, mens forespørgslen behandles. Modelserveren holder desuden en *prompt-cache* i arbejdshukommelsen, hvor starten af de seneste forespørgsler kan genbruges til at svare hurtigere. Cachen er adskilt pr. konto og overskrives løbende.
- Til afregning gemmer databehandleren pr. time, API-nøgle og model antallet af forespørgsler, tokens og pris. Disse tal indeholder ikke tekst fra input eller output.
- Databehandlerens logs indeholder tidspunkt, konto, nøgle, model, status og antal tokens, aldrig teksten i en forespørgsel eller et svar.

Ingen hos databehandleren læser input eller output. Behandlingen er fuldt automatiseret.

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

Den dataansvarlige bestemmer selv indholdet af sit input. Det kan derfor omfatte enhver type personoplysning, som den dataansvarlige vælger at medtage, herunder:

- almindelige personoplysninger (databeskyttelsesforordningens artikel 6), fx navne, kontaktoplysninger, stillinger, kundeforhold, korrespondance, notater og dokumenter
- følsomme personoplysninger (artikel 9), fx helbredsoplysninger, hvis den dataansvarlige medtager dem
- oplysninger om strafbare forhold (artikel 10) og personnumre (databeskyttelseslovens § 11), hvis den dataansvarlige medtager dem.

Den dataansvarlige er ansvarlig for, at der er hjemmel til at behandle de oplysninger, den dataansvarlige medtager i sit input, og bør ikke medtage flere personoplysninger, end formålet kræver.

### A.4. Behandlingen omfatter følgende kategorier af registrerede

De personer, der optræder i den dataansvarliges input, fx:

- den dataansvarliges medarbejdere og brugere af den dataansvarliges egne systemer
- den dataansvarliges kunder, leverandører, samarbejdspartnere og borgere
- andre personer, der nævnes i de tekster og dokumenter, den dataansvarlige sender til tjenesten.

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

Behandlingen af en forespørgsel varer, indtil svaret er sendt til den dataansvarlige. Herefter findes input og output ikke længere hos databehandleren, bortset fra prompt-cachen i modelserverens arbejdshukommelse, som overskrives løbende og tømmes, når serveren genstartes. Behandlingen kan finde sted, så længe den dataansvarlige har en konto til Dansk LLM, og ophører, når kontoen lukkes.

# Bilag B Underdatabehandlere

## B.1. Godkendte underdatabehandlere

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

| NAVN | CVR | ADRESSE | BEHANDLING |
|---|---|---|---|
| PDC A/S | 78806117 | H. J. Holst Vej 3, 5c, 2605 Brøndbyøster, Danmark | Datacenter: fysisk placering, strøm, køling og netværksforbindelse for databehandlerens egne servere (gateway, platform og GPU-servere). Serverne ejes og administreres af databehandleren. PDC A/S har ikke logisk adgang til serverne eller til de personoplysninger, der behandles på dem. |

Databehandleren bruger ingen eksterne sprogmodeltjenester eller cloudtjenester til at behandle input og output. Sprogmodellen kører på databehandlerens egne servere i datacentret ovenfor.

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandler for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarliges skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

## B.2. Varsel for godkendelse af underdatabehandlere

Databehandleren har en generel skriftlig godkendelse til at anvende underdatabehandlere, jf. Bestemmelse 7.3. Databehandleren underretter den dataansvarlige om nye eller ændrede underdatabehandlere med mindst 30 dages varsel pr. e-mail til den dataansvarliges kontaktperson og ved at opdatere listen på docs.danskllm.dk. Gør den dataansvarlige indsigelse inden fristen, og kan parterne ikke finde en løsning, kan den dataansvarlige lukke sin konto, hvorefter ubrugt købt kredit refunderes.

# 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:

- modtager den dataansvarliges input via API'et eller playgrounden, kontrollerer API-nøgle og saldo og sender input til sprogmodellen på databehandlerens egne servere
- genererer output med sprogmodellen og sender det til den dataansvarlige
- sletter input og output fra arbejdshukommelsen, når forespørgslen er afsluttet, bortset fra prompt-cachen, som overskrives løbende
- registrerer antal forespørgsler, tokens og pris til afregning, uden indhold fra input eller output.

Databehandleren må ikke gemme input eller output, lade mennesker læse dem, bruge dem til at træne eller forbedre modeller eller bruge dem til andre formål end at levere tjenesten.

## C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle, at den dataansvarlige kan medtage følsomme personoplysninger og personnumre i sit input, og at databehandleren ikke kan se eller styre, hvad input indeholder. Der skal derfor etableres et højt sikkerhedsniveau for fortroligheden af input og output under behandlingen. Risikoen for tilgængelighed og integritet er begrænset, fordi databehandleren ikke opbevarer den dataansvarliges oplysninger.

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

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

- **Kryptering under transmission:** Al trafik mellem den dataansvarlige og tjenesten er krypteret med TLS (HTTPS). Trafik mellem databehandlerens servere går over et privat netværk i datacentret.
- **Ingen opbevaring:** Input og output skrives ikke til disk, databaser, logs eller fejlrapportering. Fejlrapporter indeholder kun tekniske oplysninger (tidspunkt, konto-id, forespørgsels-id, fejltype).
- **Adskillelse mellem kunder:** Hver forespørgsel behandles isoleret. Prompt-cachen på modelserverne er adskilt pr. konto med en kontospecifik nøgle, så en konto aldrig kan ramme en anden kontos cache.
- **Adgangskontrol:** GPU-serverne kan kun nås fra databehandlerens router. Administrativ adgang til serverne kræver personlige nøgler og er begrænset til databehandlerens driftsansvarlige. Adgang til administrationen af platformen kræver totrinsbekræftelse. API-nøgler opbevares kun som hash.
- **Logning:** Logs indeholder tidspunkt, konto, nøgle, model, status og antal tokens. Logs gemmes højst 90 dage.

- **Opdatering og hærdning:** Styresystemer, containere og modelsoftware holdes opdateret med sikkerhedsrettelser. Versioner er fastlåst og ændres kontrolleret.
- **Fysisk sikkerhed:** Serverne står i et aflåst datacenter hos PDC A/S med adgangskontrol. Databehandlerens kontor bruges kun til fjernadministration.
- **Hjemme-/fjernarbejdspladser:** Fjernadministration sker fra databehandlerens egne, krypterede computere over krypterede forbindelser.
- **Genopretning:** Platformens database (konti, nøgler, saldi, forbrugstal) sikkerhedskopieres dagligt. Sikkerhedskopierne indeholder ikke input eller output, fordi de ikke gemmes. De opbevares krypteret hos Amazon Web Services EMEA SARL i Stockholm, Sverige, i et lager, hvor de ikke kan ændres eller slettes i 90 dage, og slettes automatisk efter 91 dage.
- **Afprøvning:** Databehandleren tester sikkerhedsmekanismerne i sin automatiske testsuite ved hver ændring og gennemgår sikkerheden mindst én gang om året.
- **Beredskab:** Databehandleren har en procedure for håndtering af sikkerhedshændelser, så den dataansvarlige kan underrettes inden for fristen i Bestemmelse 10.2.

## 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:

- **De registreredes rettigheder:** Fordi databehandleren ikke opbevarer input eller output, kan databehandleren ikke finde, udlevere, rette eller slette oplysninger om en bestemt registreret. Databehandlerens bistand består i at bekræfte dette skriftligt over for den dataansvarlige og at oplyse, hvilke afregningsdata der findes på kontoen, hvis den dataansvarlige beder om det.
- **Brud på persondatasikkerheden:** Databehandleren underretter den dataansvarlige pr. e-mail inden for fristen i Bestemmelse 10.2 med de oplysninger, der er nævnt i Bestemmelse 10.3, i det omfang de kendes: hvad der er sket, hvornår, hvilke konti og forespørgsler der kan være berørt, de sandsynlige konsekvenser og de foranstaltninger, databehandleren har truffet. Databehandleren supplerer, efterhånden som der kommer flere oplysninger.
- **Konsekvensanalyser:** Databehandleren stiller på forespørgsel en beskrivelse af tjenestens dataflow og sikkerhedsforanstaltninger til rådighed, så den dataansvarlige kan udarbejde en konsekvensanalyse. Beskrivelsen findes også på docs.danskllm.dk.

Bistand ud over det ovenstående kan aftales særskilt og kan faktureres efter medgået tid.

## C.4. Opbevaringsperiode/sletterutine

Input og output opbevares ikke. De slettes fra arbejdshukommelsen, når forespørgslen er afsluttet. Prompt-cachen overskrives løbende og tømmes senest ved genstart af modelserveren.

Ved ophør af tjenesten vedrørende behandling af personoplysninger er der derfor ingen personoplysninger at slette eller tilbagelevere, og databehandleren bekræfter dette over for den dataansvarlige, jf. Bestemmelse 11.1. Afregningsdata (antal forespørgsler, tokens og pris) opbevares i 5 år efter bogføringsloven. De indeholder ikke personoplysninger om de registrerede.

## 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:

- PDC A/S, H. J. Holst Vej 3, 5c, 2605 Brøndbyøster, Danmark (underdatabehandler): datacenter, hvor databehandlerens servere står, og hvor al behandling af input og output finder sted.
- Gavn Software ApS, Ulrikkenborg Allé 23, 1. th., 2800 Kongens Lyngby, Danmark (databehandleren): fjernadministration af serverne. Der behandles ikke input eller output på denne lokalitet.

## C.6. Instruks vedrørende overførsel af personoplysninger til tredjelande

Den dataansvarlige instruerer ikke databehandleren i at overføre personoplysninger til tredjelande eller internationale organisationer. Al behandling finder sted i Danmark.

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

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

Den dataansvarlige kan én gang om året og derudover ved begrundet mistanke om brud på Bestemmelserne føre tilsyn med databehandleren. Tilsynet gennemføres som udgangspunkt på skriftligt grundlag: Databehandleren besvarer den dataansvarliges spørgsmål og fremlægger relevant dokumentation (beskrivelse af dataflow og sikkerhedsforanstaltninger, oversigt over adgange, dokumentation for opdateringer og hændelser) inden for 30 dage efter anmodning.

Den dataansvarlige eller en repræsentant for den dataansvarlige kan derudover med mindst 30 dages skriftligt varsel foretage en fysisk inspektion af de systemer, der benyttes til behandlingen, i det omfang datacentret tillader det. Inspektionen skal gennemføres på hverdage i normal arbejdstid og uden unødig forstyrrelse af driften. Den dataansvarlige afholder selv sine udgifter til inspektionen. Databehandleren afsætter den tid, der er nødvendig for, at den dataansvarlige kan gennemføre inspektionen.

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.

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

Databehandleren indhenter én gang om året dokumentation fra PDC A/S for datacentrets fysiske sikkerhed og adgangskontrol, fx en revisionserklæring, en certificering eller en beskrivelse af sikkerhedsforanstaltningerne, og gennemgår den. Dokumentationen sendes til den dataansvarlige, hvis den dataansvarlige beder om det.

Den dataansvarlige kan anfægte rammerne for dokumentationen og kan i så fald anmode databehandleren om at indhente yderligere oplysninger fra underdatabehandleren. Fysisk inspektion hos underdatabehandleren kan aftales, i det omfang underdatabehandleren tillader det. Den

dataansvarliges eventuelle deltagelse ændrer ikke ved, at databehandleren har det fulde ansvar for underdatabehandlerens overholdelse af Bestemmelserne.

# Bilag D Parternes regulering af andre forhold

1. **Sammenhæng med vilkårene.** Disse Bestemmelser er en del af aftalen om Dansk LLM og supplerer Vilkår for Dansk LLM ("Vilkårene"). Ved modstrid om behandling af personoplysninger har Bestemmelserne forrang, jf. Bestemmelse 2.4. I alle andre forhold gælder Vilkårene.

2. **Erstatningsansvar.** Parternes erstatningsansvar over for hinanden i anledning af disse Bestemmelser er reguleret af Vilkårenes bestemmelser om ansvar og ansvarsbegrænsning. Ansvarsbegrænsningen gælder ikke for ansvar, der følger direkte af databeskyttelsesforordningens artikel 82, og begrænser ikke de registreredes rettigheder.

3. **Oplysninger om kontoen.** Databehandleren er selvstændigt dataansvarlig for de personoplysninger, der er nødvendige for at drive kontoen og opkræve betaling: e-mailadresse, adgangskode (som hash), oplysninger til totrinsbekræftelse, saldo, forbrugstal og betalingsoplysninger. Den behandling er beskrevet i privatlivspolitikken for Dansk LLM og er ikke omfattet af disse Bestemmelser.

4. **Ulovlige instrukser.** Hvis den dataansvarlige giver en instruks, som databehandleren vurderer er i strid med databeskyttelsesretten, jf. Bestemmelse 4.2, kan databehandleren undlade at følge instruksen, indtil parterne har afklaret spørgsmålet. Den dataansvarlige bærer ansvaret for følgerne af en instruks, som databehandleren har fulgt efter at have gjort indsigelse skriftligt.

5. **Ændringer.** Databehandleren kan opdatere bilag A–D, når tjenesten ændres, med mindst 30 dages varsel pr. e-mail og ved at offentliggøre den nye version på docs.danskllm.dk. Ændringer må ikke forringe beskyttelsen af de registrerede. Kan den dataansvarlige ikke acceptere en ændring, kan den dataansvarlige lukke sin konto, hvorefter ubrugt købt kredit refunderes.

6. **Sprog.** Bestemmelserne findes på dansk. Udarbejdes der en oversættelse, har den danske version forrang.