S Y N T A S

Databehandleraftale

Version 3.1 · 1. november 2026

Denne databehandleraftale danner grundlaget for behandling af persondata, som Syntas foretager på vegne af dig som kunde. Databehandleraftalen træder i kraft og godkendes af dig som kunde, inden du opretter stamdata i systemet.

Denne databehandleraftale er udarbejdet som standardkontraktsbestemmelser i henhold til artikel 28, stk. 3, i forordning (EU) 2016/679 (databeskyttelsesforordningen, "GDPR") med henblik på databehandlerens (Syntas) behandling af personoplysninger på vegne af dig som kunde.

1. Parterne

1.1. Databehandleren er Syntas ApS, CVR-nr. 46689046, Teglbækvej 10, 8361 Hasselager. Kontakt vedrørende databeskyttelse: kontakt@syntas.dk.

1.2. Den dataansvarlige er den virksomhed, der er oprettet som organisation i Syntas, og på hvis vegne aftalen godkendes i systemet under Indstillinger. Godkendelsen kan alene foretages af en bruger med administratorrettigheder i den pågældende organisation.

1.3. Ved godkendelsen registrerer databehandleren organisationens navn, den godkendende brugers brugernavn og fulde navn, hvilken version af aftalen der blev godkendt, samt tidspunkt, IP-adresse og browseroplysninger. Registreringen udgør parternes dokumentation for, hvem der har indgået aftalen og hvornår.

1.4. Oplysningerne gemmes som øjebliksbillede på godkendelsestidspunktet. Skifter organisationen efterfølgende navn, eller slettes den godkendende bruger, forbliver registreringen uændret.

1.5. Udgives en ny version af aftalen, bortfalder den hidtidige godkendelse ikke, men den dataansvarlige skal godkende den nye version, før behandlingen fortsætter på det nye grundlag. Tidligere godkendelser bevares som dokumentation for, hvad der var gældende indtil da.

1.6. Parterne benævnes samlet "parterne".

2. Præambel

2.1. Aftalen regulerer databehandlerens behandling af personoplysninger på vegne af den dataansvarlige i forbindelse med levering, drift, vedligeholdelse og support af Syntas, herunder tidsregistrering, projektregistrering, fravær, vagtplanlægning og personaleadministration.

2.2. Databehandleren må alene behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige og i overensstemmelse med denne aftale.

2.3. Den dataansvarlige bestemmer formålet med behandlingen og hvilke personoplysninger, der indtastes eller genereres i Syntas.

2.4. Aftalen har forrang for andre aftaler mellem parterne, i det omfang sådanne aftaler regulerer behandling af personoplysninger i strid med denne aftale.

3. Den dataansvarliges ansvar

3.1. Den dataansvarlige er ansvarlig for, at behandlingen sker i overensstemmelse med GDPR og anden gældende databeskyttelseslovgivning, herunder:

- at der foreligger et lovligt behandlingsgrundlag,
- at de registrerede modtager de oplysninger, de har krav på,

- at personoplysningerne er korrekte og relevante, og
- at instrukser til databehandleren er lovlige.

4. Databehandlerens behandling

4.1. Databehandleren må alene behandle personoplysninger for at levere, drive, vedligeholde og supportere Syntas og i øvrigt efter den dataansvarliges dokumenterede instrukser.

4.2. Databehandleren skal uden unødig forsinkelse underrette den dataansvarlige, hvis en instruks efter databehandlerens opfattelse er i strid med gældende databeskyttelseslovgivning.

4.3. Hvis databehandleren efter EU-ret eller national ret er forpligtet til at behandle personoplysninger på anden måde, skal databehandleren, medmindre lovgivningen forbyder det, underrette den dataansvarlige herom.

5. Fortrolighed og adgang

5.1. Databehandleren skal sikre, at personer, der er autoriserede til at behandle personoplysninger, er underlagt en fortrolighedsforpligtelse eller passende lovbestemt tavshedspligt.

5.2. Adgang til personoplysninger begrænses til personer, for hvem adgangen er nødvendig for at udføre deres arbejdsopgaver.

5.3. Fortrolighedsforpligtelsen gælder også efter ophør af ansættelsesforholdet og denne aftale.

6. Behandlingssikkerhed

6.1. Databehandleren skal gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger i overensstemmelse med GDPR artikel 32 og under hensyntagen til behandlingens karakter og de risici, behandlingen indebærer.

6.2. Sikkerhedsforanstaltningerne omfatter som minimum:

- krypteret kommunikation mellem klienter og servere,
- passende adgangskontrol og rettighedsstyring,
- sikker håndtering af adgangskoder,
- autentifikation og mulighed for flerfaktorgodkendelse,
- relevant logning og håndtering af sikkerhedshændelser,
- sikkerhedskopiering og mulighed for gendannelse, samt
- løbende vurdering og forbedring af sikkerhedsforanstaltninger.

6.3. De nærmere tekniske og organisatoriske foranstaltninger fremgår af bilag B.

6.4. Databehandleren skal løbende vurdere, om foranstaltningerne er passende i forhold til de risici, der er forbundet med behandlingen.

7. Underdatabehandlere

7.1. Ved godkendelse af denne databehandleraftale giver den dataansvarlige den generelle skriftlige accept til databehandleren af at anvende de underdatabehandlere, som fremgår af bilag C.

7.2. Databehandleren sikrer, at de underdatabehandlere som benyttes, også overholder de forpligtelser og krav, som er beskrevet i denne databehandleraftale.

7.3. Databehandleren underretter den dataansvarlige mindst 14 dage før anvendelse af en ny underdatabehandler eller udskiftning af en eksisterende.

7.4. Den dataansvarlige kan gøre indsigelse mod ændringen, hvis der foreligger rimelige og dokumenterede databeskyttelsesmæssige grunde.

7.5. Hvis parterne ikke kan finde en løsning på indsigelsen, kan den dataansvarlige opsige den berørte tjeneste med et forkortet varsel.

7.6. Databehandleren er ansvarlig over for den dataansvarlige for sine underdatabehandleres behandling af personoplysninger.

8. Overførsel til tredjelande

8.1. Personoplysninger må kun overføres til tredjelande eller internationale organisationer, når betingelserne i GDPR kapitel V er opfyldt.

8.2. De underdatabehandlere, der indebærer overførsel til tredjelande, samt det anvendte overførselsgrundlag, fremgår af bilag C.

8.3. Databehandleren skal sikre, at der foreligger et gyldigt overførselsgrundlag, herunder EU-Kommissionens standardkontraktbestemmelser (SCC), hvor dette er nødvendigt.

9. Bistand til den dataansvarlige

9.1. Databehandleren skal under hensyntagen til behandlingens karakter bistå den dataansvarlige med at opfylde sine forpligtelser efter GDPR, herunder vedrørende registreredes rettigheder, behandlingssikkerhed, persondatabrud, konsekvensanalyser og eventuel forudgående høring af tilsynsmyndigheden.

9.2. Databehandleren skal så vidt muligt stille funktionalitet til rådighed for, at den dataansvarlige kan søge indsigt i, berigtige, eksportere og slette personoplysninger.

9.3. Kan en anmodning ikke imødekommes gennem systemets egne funktioner, yder databehandleren bistand inden for 10 arbejdsdage efter skriftlig anmodning.

9.4. Hvis databehandleren modtager en henvendelse fra en registreret vedrørende personoplysninger, skal den dataansvarlige underrettes uden unødig forsinkelse.

9.5. Bistand, der ligger væsentligt ud over databehandlerens lovpligtige bistand, kan efter aftale faktureres særskilt.

10. Persondatabrud

10.1. Databehandleren skal underrette den dataansvarlige uden unødig forsinkelse efter at være blevet bekendt med et brud på persondatasikkerheden.

10.2. Underretningen skal, hvor det er muligt, ske senest 24 timer efter, at databehandleren er blevet bekendt med bruddet.

10.3. Underretningen skal indeholde de oplysninger, som er tilgængelige for databehandleren og nødvendige for, at den dataansvarlige kan vurdere og håndtere bruddet.

10.4. Databehandleren skal bistå den dataansvarlige med håndtering og eventuel anmeldelse af bruddet.

11. Sletning og returnering

11.1. Ved ophør af tjenesten skal databehandleren efter den dataansvarliges valg enten tilbagelevere personoplysningerne i et almindeligt anvendt format eller slette dem. Hvis den dataansvarlige ønsker, at databehandleren foretager eksporten, kan dette ske mod et gebyr.

11.2. Databehandleren skal slette eksisterende kopier, medmindre opbevaring er påkrævet efter lovgivningen.

11.3. Sletning sker senest 100 dage efter ophør, medmindre andet følger af bilag A eller lovgivningen.

11.4. Den dataansvarlige kan under aftalens løbetid eksportere sine data fra Syntas i et almindeligt anvendt format.

12. Dokumentation og revision

12.1. Databehandleren skal stille de oplysninger til rådighed, som er nødvendige for at dokumentere overholdelse af GDPR artikel 28.

12.2. Den dataansvarlige har ret til at gennemføre eller lade gennemføre revisioner, når dette er nødvendigt for at dokumentere overholdelsen af aftalen.

12.3. Databehandleren råder ikke over en ISAE 3000-erklæring eller tilsvarende uafhængig revisionserklæring. Den dataansvarlige kan i stedet anmode om skriftlig dokumentation for de gennemførte tekniske og organisatoriske foranstaltninger, herunder for de underdatabehandlere der er anført i bilag C.

12.4. Relevant, uafhængig revisionserklæring eller tilsvarende dokumentation kan efter aftale anvendes som grundlag for vurderingen.

12.5. Databehandleren skal bistå ved revisioner og inspektioner i nødvendigt omfang.

12.6. Databehandleren kan opkræve betaling for bistand, der går væsentligt ud over, hvad der følger af GDPR eller denne aftale.

13. Ændringer

13.1. Databehandleren kan ændre aftalen, hvis det er nødvendigt som følge af ændringer i lovgivning, praksis, sikkerhedsforanstaltninger eller databehandlerens behandling.

13.2. Væsentlige ændringer varsles skriftligt mindst 30 dage før ikrafttræden, medmindre en kortere frist er nødvendig af sikkerheds- eller lovgivningsmæssige årsager.

13.3. Ændringer af underdatabehandlere reguleres særskilt af punkt 7.

14. Varighed, lovvalg og værneting

14.1. Aftalen træder i kraft samtidig med hovedaftalen eller ved parternes accept og gælder, så længe databehandleren behandler personoplysninger på vegne af den dataansvarlige.

14.2. Ansvar og eventuelle begrænsninger af ansvar reguleres af hovedaftalen mellem parterne.

14.3. Aftalen er underlagt dansk ret.

14.4. Eventuelle tvister afgøres ved Byretten i Aarhus.

Bilag A — Oplysninger om behandlingen

A.1 Formål

Databehandleren behandler personoplysninger med henblik på at levere, drive, vedligeholde og supportere Syntas.

A.2 Behandlingens karakter

Behandlingen omfatter herunder, men ikke begrænset til: indsamling, registrering, opbevaring, organisering, ændring, søgning, sammenstilling, visning, eksport og sletning.

A.3 Typer af personoplysninger

- Navn, e-mailadresse, telefonnummer og adresse.
- Medarbejdernummer, stilling, afdeling, kontrakttype og ansættelsesform.
- Fødselsdato, køn, ansættelsesdato og eventuel slutdato.

- Løn- og pensionsoplysninger, hvor funktionaliteten anvendes.
- Arbejdstid, pauser, overtid, ferie- og afspadseringssaldi.
- Kørselsregistreringer, herunder fra- og til-adresser.
- Udlæg og vedhæftede bilag.
- Beskeder, kommentarer og tilmeldinger.
- Tekniske identifikatorer og enhedsoplysninger.

Der behandles som udgangspunkt ikke CPR-numre.

Fraværsoplysninger kan efter omstændighederne udgøre oplysninger om helbred efter GDPR artikel 9, afhængigt af hvordan fraværstyper navngives og anvendes.

A.4 Kategorier af registrerede

- Den dataansvarliges medarbejdere, herunder timelønnede, funktionærer, lærlinge og vikarer.
- Ledere, godkendere og administratorer.
- Kontaktpersoner hos den dataansvarliges kunder, hvor disse registreres.
- Tidligere medarbejdere, i det omfang historik bevares.

A.5 Behandlingens varighed og opbevaring

Behandlingen påbegyndes ved aftalens ikrafttræden og fortsætter, indtil den dataansvarlige ophører med at anvende Syntas. Sletning eller returnering sker herefter i overensstemmelse med punkt 11.

Den dataansvarlige er efter bogføringsloven forpligtet til at opbevare regnskabsmateriale, herunder bilag på udlæg og kørsel, i 5 år fra udgangen af det regnskabsår materialet vedrører. Det påhviler den dataansvarlige at sikre, at sådant materiale eksporteres fra Syntas inden sletning efter punkt 11. Databehandleren opbevarer ikke materiale ud over den periode, der følger af punkt 11, medmindre andet aftales skriftligt.

Bilag B — Tekniske og organisatoriske sikkerhedsforanstaltninger

Databehandleren gennemfører som minimum følgende foranstaltninger:

- HTTPS/TLS anvendes til al kommunikation mellem klienter og servere. Forbindelser omdirigeres til HTTPS, og HSTS er slået til med et års varighed.
- Session- og CSRF-cookies sendes alene over sikre forbindelser.
- Adgang til systemet kræver autentifikation. Adgangskoder opbevares alene som saltede hashværdier.
- Den dataansvarlige kan fastsætte krav til adgangskoders længde og sammensætning for sin egen organisation.
- Login spærres midlertidigt efter gentagne forkerte forsøg for at modvirke systematisk afprøvning af adgangskoder.
- Flerfaktorgodkendelse (TOTP) er tilgængelig og kan aktiveres af den enkelte bruger.
- Adgang til data er rolle- og organisationsbaseret, således at en bruger alene kan tilgå oplysninger vedrørende egen organisation og egen rolle.
- Uploadede filer opbevares adskilt fra applikationsserveren hos en objektlagringsleverandør, jf. bilag C. Adgang sker alene gennem tidsbegrænsede, signerede adresser, og filerne er ikke offentligt tilgængelige.
- Hentning af bilag logges med angivelse af hvem der har hentet hvad og hvornår.
- Ændringer af eksportstatus logges og kan tilbagerulles.
- Fejlovervågning er konfigureret uden overførsel af brugeridentitet og uden variabelværdier fra programafviklingen.
- Ændringer i kildekoden gennemgås automatisk, og udrulning sker først når automatiserede tests er bestået.

- Administrativ adgang til driftsmiljø, kildekode og domæneadministration er beskyttet med flerfaktorgodkendelse.
- Databasen sikkerhedskopieres løbende af hostingleverandøren, jf. bilag C, med mulighed for gendannelse til et vilkårligt tidspunkt inden for de seneste syv døgn.
- Gendannelse afprøves i praksis og ikke alene på papiret. Seneste gennemførte gendannelsestest er dokumenteret internt med angivelse af gendannelsestid og kontrol af, at datamængderne stemmer mellem kilde og kopi.
- Databehandleren har procedurer for håndtering af sikkerhedshændelser og persondatabrud, jf. punkt 10.
- Sikkerhedsforanstaltningerne vurderes og opdateres løbende.

Bilag C — Underdatabehandlere

Den dataansvarlige har ved godkendelse af denne aftale accepteret anvendelsen af nedenstående underdatabehandlere.

Underdatabehandler	Formål	Data og lokalitet	Overførselsgrundlag
Render Services, Inc.	Hosting af applikation og database	Al kernedata. Hostingregion: Frankfurt, Tyskland	Ikke relevant — behandling i EU. Renders databehandleraftale (render.com/dpa) er indgået
Cloudflare, Inc.	Opbevaring af uploadede filer (R2)	Bilag, kvitteringer, ansættelseskontrakter, personalehåndbøger og projektfiler. Lagringen er bundet til jurisdiktionen Den Europæiske Union	Ikke relevant — behandling i EU. Cloudflares databehandleraftale er indgået
Sentry (Functional Software, Inc.)	Fejlovervågning	Tekniske fejl- og logdata. EU-region	Databehandleraftale med EU-hosting
Brevo (Sendinblue SAS)	Transaktionsmails	Nødvendige kontakt- og systemoplysninger. EU	Ikke relevant — behandling i EU
Expo (650 Industries, Inc.)	Push-notifikationer	Enheds-token og beskedtekst. USA	EU-Kommissionens standardkontraktbestemmelser, jf. Expos vilkår
OpenStreetMap Foundation (Nominatim) og OSRM	Adresseopslag og ruteberegning	Indtastede adresser. EU og Storbritannien. Kaldes fra brugerens egen enhed	Storbritannien er omfattet af Europa-Kommissionens tilstrækkelighedsafgørelse
Anthropic, PBC	Syntas Assistent og aflæsning af bilag (Udlæg med AI Assistent). Anvendes kun, når den dataansvarlige har tilvalgt en af funktionerne	De oplysninger, der er nødvendige for at besvare en administrators spørgsmål — ikke noter og HR-oplysninger — samt billedet af et bilag, der aflæses. USA	EU-Kommissionens standardkontraktbestemmelser (2021), som er en del af Anthropics databehandlertillæg

Behandlingen af personoplysninger i Syntas sker på servere i Frankfurt, Tyskland. Overførsel til et tredjeland sker til Expo (enheds-token og beskedtekst i forbindelse med push-notifikationer) og — kun når den dataansvarlige har tilvalgt Syntas Assistent eller Udlæg med AI Assistent — til Anthropic, jf. punkt 8.

Tredjeparter, der er selvstændigt dataansvarlige: Vælger den dataansvarlige kørselsberegning via Google Maps, videregives de adresser, der indtastes på en kørselsregistrering, til Google for at finde adressen og beregne ruten. Andre oplysninger videregives ikke. Google er ikke underdatabehandler, men selvstændig dataansvarlig for Google Maps efter Googles egne vilkår. Overførsel til USA sker under EU-U.S. Data Privacy Framework. Videregivelsen sker alene på den dataansvarliges eget valg; vælges funktionen ikke, videregives intet til Google.

- Benyttes integrationer, som den dataansvarlige selv efterspørger og tilkøber, såsom løn-, ERP- eller SSO-integration, behandles data i disse tilfælde efter den dataansvarliges egen instruks i dennes eget system.
- Listen holdes opdateret.
- Tages en ny underdatabehandler i brug, underrettes den dataansvarlige efter punkt 7.