

Databehandleraftale

1.2 • 5. oktober 2026

Skabelon til en særskilt aftale mellem Cortex Solutions og den nedenfor identificerede dataansvarlige. Aftalen anvendes kun med udfyldte kundebilag A, B og C samt de her indarbejdede øvrige forhold i bilag D. Bilag beskriver den faktiske aftalte behandling; aftalen underskrives før behandling begynder.

1 Parter og dokumenter

Dataansvarlig: Kunden **[UDFYLD: fuldt juridisk navn, virksomhedsform, CVR og adresse]**. Kontaktperson for databeskyttelse og sikkerhedsbrud: **[UDFYLD: navn, funktion, e-mail og telefon med akut kontaktvej]**.

Databehandler: Cortex Solutions **[KONTROLLÉR: juridisk navn og virksomhedsform]**, CVR 34151075, Fladholm 40, 6200 Aabenraa. Databeskyttelses- og beredskabskontakt: **[UDFYLD: navn, funktion, e-mail og telefon med akut kontaktvej]**.

Parterne har aftalt nedenstående Bestemmelser for at overholde databeskyttelsesforordningen og beskytte fysiske personers rettigheder. Aftalen med bilag skal være underskrevet før import, test med virkelige personoplysninger eller anden behandling på kundens vegne. Kommerciel lancering er ikke en forudsætning for, at databehandlerforpligtelserne gælder.

Bilag A Oplysninger om behandlingen; bilag B Underdatabehandlere; bilag C Instruks og tekniske og organisatoriske sikkerhedsforanstaltninger; bilag D Øvrige forhold, nedenfor. Samtlige dokumenter: version 1.2 dateret 5. oktober 2026, med de ændringer parterne udfylder og accepterer.

2 Præambel

2.1 Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.

2.2 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).

2.3 I forbindelse med leveringen af **[UDFYLD: konkret ydelse og aftalereference]** behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

2.4 Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

2.5 Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

2.6 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.

2.7 Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.

2.8 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.

2.9 Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.

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

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

3 Den dataansvarliges rettigheder og forpligtelser

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

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

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

4 Databehandleren handler efter instruks

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

4.2 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

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

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

6 Behandlingssikkerhed

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

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

- (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.

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

6.4 Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved 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.

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

7 Anvendelse af underdatabehandlere

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

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

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

7.4 Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af 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.

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

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

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

8 Overførsel til tredjelande eller internationale organisationer

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

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

8.3 Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af 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

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

8.5 Disse Bestemmelser skal ikke forveksles med standardkontraktbestemmelser 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

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

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

9.2 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 unødigt forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

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

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

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

9.3 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

10.1 Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

10.2 Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

10.3 I overensstemmelse med Bestemmelse 9.2.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.

10.4 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

11.1 Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

11.2 Der er ved aftalens indgåelse ikke identificeret regler, som pålægger Cortex at opbevare Kundens personoplysninger efter ophør. Et senere identificeret retligt opbevaringskrav dokumenteres efter bilag C.4.

11.3 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

12.1 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.

12.2 Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.

12.3 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

13.1 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

14.1 Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.

14.2 Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller u hensigtsmæssigheder i Bestemmelserne giver anledning hertil.

14.3 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.

14.4 Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.

15 Kontaktpersoner

15.1 Parterne kan kontakte hinanden via kontaktpersonerne i punkt 1. Sikkerhedsbrud meddeles til de udfyldte akutte kontaktveje.

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

16 Underskrifter

For Kunden: **[UDFYLD: navn og stilling]** • Dato: **[UDFYLD]** • Underskrift: _____

For Cortex Solutions: **[UDFYLD: navn og stilling]** • Dato: **[UDFYLD]** • Underskrift: _____

Underskrifterne omfatter bilag A, B og C samt bilag D nedenfor. Ved særskilt elektronisk underskrift vedlægges alle bilag.

Bilag D Øvrige forhold

D.1 Cortex suspenderer en konkret instruks, der efter Cortex' vurdering er ulovlig, orienterer straks Kunden og søger afklaring. Lovlig behandling fortsætter i det omfang muligt. Kan lovlig behandling ikke etableres, kan den berørte behandling bringes til ophør; kommerciel afregning må ikke tvinge parterne til ulovlig behandling.

D.2 Kunden kan ændre valget i punkt 11.1 til sletning uden tilbagelevering ved dokumenteret instruks. Ellers gælder tilbagelevering og sletning efter C.4. Dette ændrer ikke kundens ret til at vælge efter artikel 28, stk. 3, litra g.

D.3 Almindelig aftalt sikkerhed, nødvendig standardekspert og dokumentation er inkluderet. Ekstraordinær bistand og nye kundekrav kan afregnes efter forudgående skriftlig aftale, men betaling eller manglende prisaccept må ikke hindre lovpligtig bistand, tilsyn eller opfyldelse af Bestemmelserne. Nødvendig skiftebistand følger hovedaftalens punkt 21 og må ikke faktureres som særlig migrering. Cortex betaler afhjælpning af egne mangler.

D.4 Ansvar mellem parterne følger de accepterede generelle betingelser alene i det omfang, dette ikke strider mod Bestemmelserne eller ufravigelig databeskyttelsesret. Registreredes rettigheder, lovpligtige forpligtelser og myndighedsadgang begrænses ikke.

D.5 Den valgfrie bestemmelse om Kunden som begunstiget tredjemand ved Cortex' konkurs er ikke valgt.

[JURIDISK OG LEVERANDØRKONTROL: vurder behov for direkte tilbagelevering fra hostingudbyder, adgang til eksport og kontinuitetsplan ved Cortex' ophør].

Bilag A Behandlingsaktiviteter og personoplysninger

1.2 • 5. oktober 2026

Udfyld et kundespecifikt bilag. Medtag kun faktisk aftalte aktiviteter; slet irrelevante kategorier. Behandlingsgrundlag fastlægges af kunden, og sikkerhed afstemmes med risiko og bilag C. Et åbent felt er ikke en behandlingsinstruks.

A.1 Kunde formål og varighed

Dataansvarlig: **[UDFYLD: juridisk navn, CVR, adresse og kontakt]**. Cortex er databehandler for **[UDFYLD: konkret projekt og løsninger]**. Formålet er **[UDFYLD: kundens specificerede formål]**. Aftale og versionsreference: **[UDFYLD]**. Behandlingsstart: **[UDFYLD]**. Varighed og ophør: **[UDFYLD: serviceperiode og afgrænset eksport- og sletteperiode]**. En abonnementsbinding er ikke en generel opbevaringsfrist.

Rollefordeling ved direkte kundaftaler med cloud-, betalings-, AI- eller andre leverandører: **[UDFYLD: hvem er dataansvarlig, databehandler og underdatabehandler for hver aktivitet]**. Cortex' egne faktura- og kontaktoplysninger til administration behandles som selvstændig dataansvarlig efter den relevante persondatapolitik og giver ikke adgang til at bruge løsningens kundedata til egne formål.

A.2 Aktivitetsposter

Gentag denne post for hver relevant aktivitet. Aktivitet og formål: **[UDFYLD]**. Behandlingshandlinger: **[UDFYLD: eksempelvis indsamling, import, lagring, visning, analyse, videregivelse, support, eksport og sletning]**.

Kategorier af registrerede: **[UDFYLD]**. Konkrete personoplysninger og følsomhed: **[UDFYLD]**. Kilder og modtagere: **[UDFYLD]**. Roller med adgang: **[UDFYLD]**. Omfang og frekvens: **[UDFYLD]**. Leverandør- og lokationsreference til B og C: **[UDFYLD]**. Slettefrist og udløser: **[UDFYLD]**. Kundens godkendelse: **[UDFYLD]**.

Relevante aktiviteter vælges efter løsningen: hjemmesideformularer og booking; brugerlogin; medarbejder-, kunde- eller medlemsadministration; planlægning og tidsregistrering; fravær; dokumenter, beskeder og billeder; integrationer og automatiseret overførsel; AI-indeksering, søgning og svar; drift, logs og support; mail, notifikationer og backup. Eksemplerne er ikke tilladelse til at indsamle alle disse oplysninger.

A.3 Særlige data og AI

Særlige kategorier efter artikel 9, strafbare forhold og CPR: **[UDFYLD: faktisk indhold, nødvendighed, instruks og særlige begrænsninger eller angiv ingen]**. Sygdomsregistrering kan være en helbredsoplysning selv uden diagnose. Fritekst, dokumenter og billeder vurderes konkret; undgå unødvendige følsomme oplysninger.

Ved AI eller dokumentassistent beskrives indhold, indeks og embeddings, prompts, svar, metadata, modelleverandør, supportadgang, opbevaring og sletning af afledte oplysninger: **[UDFYLD]**. Ingen egen modeltræning, salg af data eller udvidelse til andre formål er instrueret. Kontrol af adgang ved søgning og svar: **[UDFYLD]**. Beslutninger om personer og eventuel profilering: **[UDFYLD eller angiv ingen; nye formål kræver særskilt instruks og vurdering]**.

A.4 Test opbevaring og godkendelse

Test foretages med syntetiske eller effektivt anonymiserede data. Virkelige data kræver dokumenteret nødvendighed, godkendt instruks og passende beskyttelse. Sletteplanen dækker produktion, lokale kopier, testsystemer, supportsager, logning, vedhæftninger, AI-indeks og backup. Ved gendannelse genanvendes tidligere sletteinstrukser. Konkrete frister og kontrol: **[UDFYLD]**.

Kunden fastlægger lovligt behandlingsgrundlag og vurderer behovet for konsekvensanalyse; Cortex yder den aftalte og lovpligtige bistand. Databehandleraftalen er ikke selv behandlingsgrundlag. Kundens godkendelse af bilag: **[UDFYLD: navn, dato, version]**. Cortex' kontrol af afgrænsning og teknisk gennemførlighed: **[UDFYLD]**.

Bilag B Underdatabehandlere

1.2 • 5. oktober 2026

Dette kundespecifikke register indeholder de faktisk godkendte leverandører og lokationer. Udfyld og godkend før adgang til data. Softwarekøb uden leverandøradgang til personoplysninger er ikke alene en underdatabehandlerrelation.

B.1 Godkendte leverandører

[UDFYLD: en fuldstændig post for hver juridisk leverandør, herunder relevante videre underdatabehandlere. Medtag hosting, database, filopbevaring, backup, logning og overvågning, e-mail/push, supportværktøj og eksterne udviklere med adgang. Slet irrelevante poster. En leverandør skal ikke medtages alene fordi Cortex køber software uden adgang til kundedata].

Registerpost som gentages for hver leverandør

Juridisk navn: **[UDFYLD]** • CVR/registreringsnummer: **[UDFYLD]** • Registreret adresse og land: **[UDFYLD]**.

Tjeneste og konkret behandlingsaktivitet: **[UDFYLD]**. Personoplysninger og kategorier af registrerede: **[UDFYLD med henvisning til aktivitetsposter i A.2]**. Adgangens karakter: **[UDFYLD: lagring, administration, support, transmission mv.]**.

Primær lagring og behandling: **[UDFYLD: land, region og relevant datacenter/lokalitet]**. Backup og katastrofeberedskab: **[UDFYLD: lande og regioner]**. Support, fjernadgang og administration: **[UDFYLD: alle lande, også adgang uden for EU/EØS]**.

Videre underdatabehandlere: **[UDFYLD: juridiske navne, funktioner og lokationer; vedlæg dateret liste]**. Leverandørens databehandleraftale og dokumentation: **[UDFYLD: reference, version, dato og opbevaringssted]**.

Tredjelandsoverførsel: **[UDFYLD: ja/nej og faktiske modtagere, lande, data og adgangstyper]**. Overførselsgrundlag og dokumentation: **[UDFYLD: konkret artikel 45-afgørelse eller artikel 46-grundlag, eventuelt SCC-modul, TIA og supplerende foranstaltninger]**. Godkendt instruks: henvisning til C.6 **[UDFYLD]**.

Sikkerhedsvurdering og tilsyn: **[UDFYLD: dato, dokumentation, ansvarlig og næste vurdering]**. Kundens godkendelse: **[UDFYLD: dato, person og versionsreference]**. Ibrugtagning: **[UDFYLD: dato]**.

B.2 Varsling og indsigelser

Der anvendes generel skriftlig godkendelse efter Bestemmelse 7. Planlagte tilføjelser og udskiftninger varsles mindst 30 kalenderdage før adgang, med alle registeroplysninger og konsekvenser for sikkerhed og lokation. Kunden kan gøre begrundet databaseskyttelsesindsigelse inden 15 kalenderdage fra modtagelse. Indsigelsesfristen er en planlægningsfrist og ophæver ikke retten til at reagere på efterfølgende væsentlige oplysninger.

Cortex og Kunden søger en forsvarlig løsning, eksempelvis alternativ leverandør eller afværgeforanstaltninger. Den omtvistede leverandør får ikke adgang, før indsigelsen er løst. Kan en nødvendig ændring ikke løses, kan begge parter bringe den berørte ydelse til ophør før ændringen uden betaling for restbinding eller tilbagebetaling af etableringsrabat. Ubestridte leverede ydelser betales; data tilbageleveres og slettes efter C.4.

B.3 Ajourføring og lokationer

Cortex holder listen dateret og versionsstyret og sender ændringer til Kundens kontaktperson. Ændring af behandlingsaktivitet eller adgangsland hos en eksisterende leverandør behandles som en væsentlig ændring og kræver de relevante instrukser og godkendelser. Et link til en ubestemt dynamisk leverandørliste erstatter ikke den aftalte liste.

EU-lagring dokumenterer ikke i sig selv, at al behandling sker i EU/EØS. Cortex kortlægger supportadgang, administration, logs, backups og videre leverandører. Ændring af lokalitet kræver den forudgående godkendelse efter C.5, og tredjelandsbehandling kræver instruks efter C.6.

B.4 Leverandøraftaler og dokumentation

Cortex sikrer bindende aftaler med tilsvarende databeskyttelsesforpligtelser og dokumenteret sikkerhed, sletning, hændelsesrapportering og tilsyn. Relevant databeskyttelsesindhold udleveres til Kunden efter anmodning; uvedkommende kommercielle forhold kan udelades. Cortex forbliver ansvarlig for underdatabehandlernes forpligtelser efter hovedaftalen.

[KONTROL FØR UNDERSKRIFT: bekræft at alle registerposter er udfyldt; afstem faktiske systemindstillinger med lokationer; vedlæg relevante lister og dokumentation; få Kundens godkendelse. Ingen faktisk leverandør er antaget eller navngivet i dette bilag].

Bilag C Instruks og sikkerhedsforanstaltninger

1.2 • 5. oktober 2026

Udfyld bilaget til det konkrete projekt. De angivne sikkerhedskrav er kontraktkrav, ikke en erklæring om eksisterende teknik. Cortex dokumenterer implementering før relevant behandling. Risiko, data og leverance afstemmes med bilag A. Lokationer, overførsler og sletning skal være afklaret.

C.1 Dokumenteret instruks

Cortex instrueres alene i at udføre de udfyldte aktiviteter i bilag A for den aftalte løsning. Behandling omfatter kun de aftalte data, formål og autoriserede brugere. Supportadgang begrænses og logges. Nye datafelter, formål, modtagere eller AI-leverandører kræver relevant ny instruks og godkendelse.

Efterfølgende instrukser gives skriftligt af **[UDFYLD: autoriserede kontaktpersoner]** og opbevares sammen med aftalen. Nye risici eller datatyper vurderes før ændringen. Kundens almindelige brug inden for bilag A er en del af instruksen, men kan ikke i sig selv godkende en ny leverandør eller tredjelandsoverførsel.

C.2 Risikovurdering og minimumssikkerhed

Risikovurderingen omfatter de faktisk aftalte oplysninger og risici for uautoriseret adgang, ændring, tab og utilgængelighed. Følsomme oplysninger begrænses til nødvendige roller. **[UDFYLD: dateret risikovurdering, arkitektur, omfang, sikkerhedsansvarlig og kundens vurdering af behov for konsekvensanalyse]**.

Identitet og adgang: individuelle konti; mindst mulige rettigheder; rollebaseret adgang og adskillelse mellem kunders data; multifaktorautentifikation for Cortex' administrative adgang; sikker nulstilling; ingen delte administratorkonti. Rettigheder gennemgås mindst kvartalsvis og ved rolleændring. Adgang fjernes straks ved ophørt arbejdsbetinget behov. **[UDFYLD: loginløsning, roller og kunde-MFA]**.

Kryptering: TLS 1.2 eller nyere for transmission; kryptering af databaser, lagrede filer og backups; adskilt og begrænset nøgleadgang; adgangskoder lagres kun som sikre saltede hashes, hvis egne passwords bruges. **[UDFYLD: teknologier, nøgleforvaltning, rotationsprocedure og dokumentation]**.

Drift og systembeskyttelse: sikre konfigurationer, begrænsede netværksporte, adskilte produktions- og testmiljøer, opdaterede enheder, overvågning og beskyttelse af hemmeligheder uden for kode. Kritiske sårbarheder risikovurderes straks og afhjælpes eller afværges uden unødigt forsinkelse. **[UDFYLD: patchfrister, scanningsfrekvens og ansvarlig]**.

C.2 Minimumssikkerhed fortsat

Backup og gendannelse: Når Cortex har ansvar for hosting eller backup af kundedata, omfatter automatiske backups de aftalte databaser, filer og nødvendige konfigurationer. Kopier beskyttes mod uautoriseret adgang, utilsigtet sletning og samtidige fejl i produktion. Fejl opdages og følges op. Gendannelse afprøves mindst kvartalsvis og efter væsentlige arkitekturændringer med dokumenteret resultat. Ved direkte kundedrift fastlægges ansvar og kontrol konkret; Cortex opretter ikke unødvendige egne datakopier. **[UDFYLD: ansvarsfordeling, faktisk omfang og dokumentation]**.

[UDFYLD OG GODKEND FØR BEHANDLING: backupfrekvens for database og filer; backupretention; separat lokation og adgangsbeskyttelse; maksimalt accepteret datatab i tid (RPO); mål for gendannelsestid (RTO); procedure for gendannelse; testansvarlig. RPO/RTO må ikke oplyses som garantier uden særskilt SLA].

Logning og overvågning: administrative login, adgang til følsomme oplysninger, væsentlige dataændringer, eksport og sikkerhedshændelser logges i relevant omfang med bruger og tidspunkt. Logs beskyttes mod manipulation og uautoriseret adgang. Personoplysninger og indhold i logs minimeres. **[UDFYLD: hændelsestyper, opbevaringsperiode, alarmer, kontrolhyppighed og adgangsroller]**.

Udvikling og ændringer: versionsstyring, faglig gennemgang af væsentlige ændringer, sikkerhedstest og afprøvning før produktionssætning samt dokumenteret tilbageførsplan. Testdata er syntetiske eller

anonymiserede, medmindre nødvendig persondatatest er særskilt instrueret. Ingen personoplysninger eller kodehemmeligheder sendes til AI-tjenester uden særskilt afklaring af instruks, leverandør og overførsel.

Organisation, fysisk sikkerhed og fjernarbejde: fortrolighedsforpligtelse, introduktion og løbende sikkerhedsopklaring; arbejdsbetinget adgang; krypterede opdaterede arbejdscomputere, skærmlås og sikker fjernadgang. Datacenterleverandørens fysiske adgang og miljøsikring dokumenteres. Lokale kopier begrænses og slettes efter opgaven. **[UDFYLD: ansvarlige, procedurer og dokumentation]**.

Evaluerings: sikkerhedsforanstaltninger vurderes mindst årligt og efter væsentlige ændringer eller hændelser. Afvigelser dokumenteres med ansvarlig og frist. Kundens nødvendige yderligere foranstaltninger aftales og dokumenteres; lovpligtige eller nødvendige foranstaltninger kan ikke udsættes alene af hensyn til pris.

C.3 Bistand og håndtering af brud

Rettighedsanmodninger modtaget af Cortex videresendes til Kunden uden unødigt forsinkelse, normalt inden 2 arbejdsdage. Cortex bistår med søgning, sikker eksport, berigtigelse, begrænsning og sletning samt med databeskyttelse, risikovurdering, konsekvensanalyse og forudgående høring, under hensyn til behandlingens karakter og oplysninger til rådighed. Kunden afgør anmodninger og lovlig opbevaring.

C.3 Bistand og brud fortsat

Ved et konstateret brud på persondatasikkerheden underrettes Kunden uden unødigt forsinkelse og om muligt senest 24 timer efter, at Cortex blev bekendt med bruddet. Første underretning afventer ikke fuld analyse. Cortex beskriver tidspunkt, bruddets karakter, berørte systemer, datatyper og omtrentligt antal personer/registreringer, sandsynlige konsekvenser, kontaktperson og iværksatte eller foreslåede afværgeforanstaltninger. Manglende oplysninger følger i etaper.

Cortex sikrer spor og dokumentation, begrænser skaden, koordinerer genopretning og bistår Kunden med anmeldelse og underretning af registrerede. Kunden træffer beslutninger om anmeldelse og underretning som dataansvarlig. Akutte kontaktveje skal fungere uden for supporttiden. **[UDFYLD OG TEST: beredskab, eskalation, stedfortrædere og underdatabehandlernes rapporteringsfrister]**.

C.4 Opbevaring sletning og tilbagelevering

Under drift følger Cortex de særskilte godkendte frister i A.2 og A.4. Kunden kan instruere i berigtigelse, eksport og sletning. Sletteproceduren omfatter produktionsdatabase, filer, relevante kopier, testdata og underdatabehandlere; berørte logs vurderes særskilt efter det dokumenterede formål og frist.

Ved ordinært ophør tilbyder Cortex sikker standardeksport og afklarer straks kundens valg. Uden instruks om ren sletning tilbageleveres oplysningerne senest 30 kalenderdage efter ophør i aftalt anvendeligt format med nødvendig beskrivelse. Aktive kopier slettes efter verificeret tilbagelevering eller sletteinstruks uden unødigt forsinkelse og senest 30 kalenderdage efter ophør. Ved skift efter hovedaftalens punkt 21 går den lovpligtige afhentningsperiode forud: aktive kopier bevares til afhentning mindst 30 kalenderdage efter overgangen og slettes derefter uden unødigt forsinkelse, medmindre en lovlig dokumenteret instruks kræver andet. Hele eksport- og afhentningsperioden er omfattet af aftalen.

Personoplysninger i beskyttede backups slettes ved dokumenteret rotation senest 90 kalenderdage efter sletningen af aktive kopier. De anvendes indtil da alene til nødvendig sikring. Efter gendannelse gennemføres tidligere sletninger igen før almindelig adgang. Cortex dokumenterer, at proceduren omfatter underdatabehandlere. **[TEKNISK OG JURIDISK KONTROL: bekræft konkret backuprotation og behov for kortere frister før behandling]**.

Cortex bekræfter skriftligt sletning, inklusive backupstatus og endelig rotationsdato. Hvis EU-ret eller dansk ret kræver fortsat opbevaring, oplyses konkret hjemmel, data, formål og frist til Kunden; oplysningerne adskilles og behandles kun som loven kræver. Cortex' egne faktura- og aftaleoplysninger som selvstændig dataansvarlig giver ikke adgang til at bevare hele kundens portaldata.

C.5 Behandlingslokationer

Behandling må kun ske på de lokationer, som Kunden har godkendt skriftligt i dette punkt og i bilag B. Lokation omfatter produktion, database, filer, backups, logs, support og fjernadministration.

Cortex' egen behandling: **[UDFYLD: adresse/lokaltet, land, funktion og fjernarbejdslokationer]**.
Leverandørbehandling: **[UDFYLD: henvisning til hver dateret registerpost i bilag B med lande, regioner og relevante lokaliteter]**. Ændringer kræver Kundens forudgående skriftlige godkendelse; varsling alene er ikke godkendelse af et nyt land.

C.6 Tredjelandsoverførsler

Der er ikke instrueret i tredjelandsoverførsel, før en konkret overførsel er beskrevet og accepteret her. Cortex kontrollerer både lagring og adgang fra lande uden for EU/EØS. Godkendelse af en leverandør er ikke i sig selv et overførselsgrundlag.

[UDFYLD PR. EVENTUEL OVERFØRSEL: dataeksportør og -importør; juridisk modtager og land; formål; oplysninger; adgangsform; videre modtagere; frekvens og varighed; konkret grundlag efter GDPR kapitel V; dokumentversion og dato].

Ved artikel 45 kontrolleres, at den aktuelle tilstrækkelighedsafgørelse faktisk dækker land, modtager og behandling. Ved artikel 46 dokumenteres relevant grundlag, eventuelt EU-Kommissionens standardkontraktbestemmelser med korrekt modul, transfer impact assessment og nødvendige supplerende foranstaltninger. **[JURIDISK KONTROL: konkret overførsel og grundlag før adgang]**.

Instruks godkendt af Kunden: **[UDFYLD: navn, dato og reference]**. Uden udfyldt instruks er tredjelandsoverførsel ikke tilladt. Hvis overførselsgrundlaget bortfalder eller beskyttelsen ikke længere er tilstrækkelig, standses den berørte overførsel, og parterne søger en lovlig løsning. Databehandleraftalen udgør ikke et overførselsgrundlag.

C.7 Tilsyn med Cortex

Kunden kan kræve relevante oplysninger og foretage audit eller inspektion selv eller ved en bemyndiget uafhængig revisor. En årlig dokumentgennemgang er udgangspunkt; yderligere tilsyn er muligt ved behov, hændelser, væsentlige ændringer eller myndighedskrav. Normalt varsel er 10 arbejdsdage, men forkortes ved hastende risiko eller myndighedskrav. Ingen frekvensbegrænsning må hindre nødvendigt tilsyn.

Cortex stiller dokumentation, relevante medarbejdere og adgang til relevante systemer og lokationer til rådighed. Tilsyn planlægges med hensyn til andre kunders fortrolighed og drift; dette må ikke gøre kontrollen ineffektiv. Rapporter, konstaterede afvigelser og afhjælpningsplan deles. Kunden bærer egne revisors udgifter; Cortex stiller nødvendig almindelig bistand til rådighed og betaler afhjælpning af egne mangler.

C.8 Tilsyn med underdatabehandlere

Cortex gennemfører dokumenteret sikkerheds- og aftalevurdering før adgang og mindst årligt samt ved væsentlige ændringer eller hændelser. Tilsynet baseres på behandlingens risiko, relevante rapporter, aftaler, lokationer, hændelser og faktisk konfiguration. Eventuelle ISO- eller revisionsrapporter vurderes for omfang, periode og undtagelser; en certificering alene erstatter ikke vurderingen.

Hvis dokumentation ikke er tilstrækkelig, indhenter Cortex uddybning, kræver afhjælpning og gennemfører eller organiserer nødvendig audit/inspektion. Kunden får relevante resultater og kan initiere eller deltage i nødvendigt tilsyn, herunder ved bemyndiget revisor. Cortex sikrer, at leverandøraftaler muliggør effektiv kontrol. Manglende kontraktadgang til nødvendigt tilsyn skal afklares før leverandøren tages i brug.

Cortex afholder egne og underdatabehandlernes almindelige tilsynsomkostninger. Kunden afholder egne ekstra revisors udgifter. Ingen betalingsbestemmelse begrænser artikel 28-rettigheder eller myndighedsadgang.

C.9 Dokumentation før behandling

[UDFYLD: sikkerhedsansvarlig og dato for teknisk godkendelse]. Vedlæg arkitektur- og dataflowoversigt, risikovurdering, adgangsmatrix, backup- og gendannelsestest, sletteprocedure, beredskab og leverandørdokumentation. Der er ikke angivet nogen ISO-certificering, penetrationstest eller forsikringsdækning som eksisterende forhold.

Kundens godkendelse af bilagets instruks og konkrete felter: **[UDFYLD: navn og dato]**. Cortex' bekræftelse af implementerede kontraktkrav: **[UDFYLD: navn og dato]**. Bilaget versionsstyres sammen med hovedaftalen. Åbne felter afklares før den relevante behandling påbegyndes.