

Databehandlersaftale for Saldi

Danosoft ApS · CVR 46412532

Version 30. september 2026 · Ikrafttræden ved kundens accept

Bilag 2 til Handelsbetingelser for Danosoft ApS. Aftalen fastlægger parternes rettigheder og pligter ved behandling af personoplysninger i Saldi på kundens vegne. Bilag A-D er en integreret del af aftalen.

Parter

Dataansvarlig: Kunden, som identificeret med navn, CVR-nr., adresse og kontaktoplysninger i den tilknyttede kunde-/ordrebekræftelse og registreringen af kundens accept. I aftalen benævnt "kunden" eller "den dataansvarlige".

Databehandler: Danosoft ApS, CVR-nr. 46412532, Østergade 24, 3200 Helsinge, Danmark. I aftalen benævnt "Danosoft" eller "databehandleren".

Henvendelser til Danosoft om denne aftale og persondatasikkerhed sendes til info@saldi.dk. Danosoft sender underretninger til kundens senest registrerede kontaktadresse i kundeforholdet og ved hastende forhold også til kundens øvrige tilgængelige kontaktpunkter. Parterne holder deres kontaktoplysninger ajour. En særskilt skriftligt meddelt sikkerhedskontakt anvendes, når en sådan er registreret.

1 Baggrund for databehandlersaftalen

1. Denne aftale fastsætter de rettigheder og forpligtelser, som finder anvendelse, når databehandleren foretager behandling af personoplysninger på vegne af den dataansvarlige.
2. Aftalen 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), som stiller specifikke krav til indholdet af en databehandlersaftale.
3. Databehandlerens behandling af personoplysninger sker med henblik på opfyldelse af parternes aftale om Saldi, herunder Handelsbetingelser for Danosoft ApS og eventuelle individuelle aftaler ("hovedaftalen"). Denne databehandlersaftale udgør Bilag 2 til handelsbetingelserne.
4. Databehandlersaftalen og "hovedaftalen" er indbyrdes afhængige og kan ikke opsiges særskilt. Databehandlersaftalen kan dog – uden at opsige "hovedaftalen" – erstattes af en anden gyldig databehandlersaftale.
5. Denne databehandlersaftale har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne, herunder i "hovedaftalen".
6. Til denne aftale hører fire bilag. Bilagene fungerer som en integreret del af databehandlersaftalen.
7. Databehandlersaftalens Bilag A indeholder nærmere oplysninger om behandlingen, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
8. Databehandlersaftalens Bilag B indeholder den dataansvarliges betingelser for, at databehandleren kan gøre brug af underdatabehandlere, samt en liste over de underdatabehandlere, som den dataansvarlige har godkendt.
9. Databehandlersaftalens Bilag C indeholder en nærmere instruks om, hvilken behandling databehandleren skal foretage på vegne af den dataansvarlige (behandlingens genstand), hvilke sikkerhedsforanstaltninger, der som minimum skal iagttages, samt hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
10. Databehandlersaftalens Bilag D indeholder parternes eventuelle regulering af forhold, som ikke ellers fremgår af databehandlersaftalen eller parternes "hovedaftale".
11. Databehandlersaftalen med tilhørende bilag opbevares skriftligt, herunder elektronisk af begge parter.
12. Denne databehandlersaftale frigør ikke databehandleren for forpligtelser, som efter databeskyttelsesforordningen eller enhver anden lovgivning direkte er pålagt databehandleren.

13. Danosoft er databehandler for personoplysninger i kundens regnskaber og øvrige applikationsdata, som behandles på kundens vegne. Danosofts behandling til egne, særskilt fastlagte formål, eksempelvis egen fakturering og administration af kundeforholdet, reguleres af den relevante privatlivspolitik og kræver selvstændigt behandlingsgrundlag. Brugsdata og logdata henføres til den rette rolle efter det konkrete formål; de er ikke automatisk Danosofts egne data. Denne aftale giver ikke tilladelse til egne sekundære formål.

2 Den dataansvarliges forpligtelser og rettigheder

1. Den dataansvarlige har over for omverdenen (herunder den registrerede) som udgangspunkt ansvaret for, at behandlingen af personoplysninger sker inden for rammerne af databeskyttelsesforordningen og databeskyttelsesloven.
2. Den dataansvarlige har derfor både rettighederne og forpligtelserne til at træffe beslutninger om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling.
3. Den dataansvarlige er blandt andet ansvarlig for, at der foreligger hjemmel til den behandling, som databehandleren instrueres i at foretage.
4. Behandling, som er nødvendig for at opfylde en konkret pligt efter bogføringslovgivningen, kan baseres på databeskyttelsesforordningens artikel 6, stk. 1, litra c, når betingelserne herfor er opfyldt. Bogføringspligten er ikke et generelt behandlingsgrundlag for alle oplysninger og funktioner i Saldi eller for AI-træning. Andre formål og eventuelle særlige kategorier kræver deres eget relevante behandlingsgrundlag.

3 Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art. 28, stk. 3, litra a.
2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.
3. Hovedaftalens bestemmelser om udvikling, statistik, anonymisering og brug af data udvider ikke i sig selv instruksens til at behandle kundens personoplysninger til Danosofts eller tredjemands egne formål. Anonymisering er også behandling af personoplysninger, indtil oplysningerne er reelt anonyme, og skal ske inden for en lovlig og dokumenteret ramme.

4 Fortrolighed

1. Databehandleren sikrer, at kun de personer, der aktuelt er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af den dataansvarlige. Adgangen til oplysningerne skal derfor straks lukkes ned, hvis autorisationen fratages eller udløber.
2. Der må alene autoriseres personer, for hvem det er nødvendigt at have adgang til personoplysningerne for at kunne opfylde databehandlerens forpligtelser over for den dataansvarlige.
3. Databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger på vegne af den dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.
4. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de relevante medarbejdere er underlagt ovennævnte tavshedspligt.
5. Fortrolighedsforpligtelsen gælder også efter aftalens ophør.

5 Behandlingssikkerhed

1. Databehandleren iværksætter alle foranstaltninger, som kræves i henhold til databeskyttelsesforordningens artikel 32, hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.
2. Ovenstående forpligtelse indebærer, at databehandleren skal foretage en risikovurdering, og herefter gennemføre foranstaltninger for at imødegå identificerede risici. Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:
 - 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
3. Databehandleren skal i forbindelse med ovenstående – i alle tilfælde – som minimum iværksætte det sikkerhedsniveau og de foranstaltninger, som er specificeret nærmere i denne aftales Bilag C.
4. Parternes eventuelle regulering/aftale om vederlæggelse eller lign. i forbindelse med den dataansvarliges eller databehandlerens efterfølgende krav om etablering af yderligere sikkerhedsforanstaltninger vil fremgå af parternes "hovedaftale" eller af denne aftales bilag D.

6 Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2 og 4, for at gøre brug af en anden databehandler (underdatabehandler).
2. Databehandleren må ikke anvende en underdatabehandler uden den dataansvarliges forudgående generelle skriftlige godkendelse efter bilag B.
3. Databehandleren underretter den dataansvarlige om planlagte tilføjelser og udskiftninger af underdatabehandlere efter den varslings- og indsigelsesprocedure, der er fastlagt i bilag B, og giver derved den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.
4. Den dataansvarliges nærmere betingelser for databehandlerens brug af underdatabehandlere fremgår af denne aftales Bilag B.
5. De underdatabehandlere, som den dataansvarlige har godkendt ved aftalens indgåelse, er anført i denne aftales Bilag B.
6. Når databehandleren har den dataansvarliges godkendelse til at gøre brug af en underdatabehandler, sørger databehandleren for at pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er fastsat i denne databehandlersaftale, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen.

Databehandleren er således ansvarlig for – igennem indgåelsen af en underdatabehandlersaftale – at pålægge en eventuel underdatabehandler mindst de forpligtelser, som databehandleren selv er underlagt efter databeskyttelsesreglerne og denne databehandlersaftale med tilhørende bilag.

7. Underdatabehandlersaftalen 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 der er indgået en gyldig aftale mellem databehandleren og underdatabehandleren. Eventuelle kommercielle vilkår, eksempelvis priser, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandlersaftalen, skal ikke sendes til den dataansvarlige.

8. Databehandleren skal i sin aftale med underdatabehandleren indføre den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandleren, f.eks. så den dataansvarlige kan instruere underdatabehandleren om at foretage sletning eller tilbagelevering af oplysninger.

9. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.

7 Overførsel af oplysninger til tredjelande eller internationale organisationer

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår overførsel (overladelse, videregivelse samt intern anvendelse) af personoplysninger til tredjelande eller internationale organisationer, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art. 28, stk. 3, litra a.

2. Uden den dataansvarliges instruks eller godkendelse kan databehandleren – inden for rammerne af databehandlersaftalen – derfor bl.a. ikke:

- a. videregive personoplysningerne til en dataansvarlig i et tredjeland eller i en international organisation,
- b. overlade behandlingen af personoplysninger til en underdatabehandler i et tredjeland,
- c. lade oplysningerne behandle i en anden af databehandlerens afdelinger, som er placeret i et tredjeland.

3. Den dataansvarliges eventuelle instruks eller godkendelse af, at der foretages overførsel af personoplysninger til et tredjeland, vil fremgå af denne aftales Bilag C.

4. Instruks eller godkendelse erstatter ikke kravene til et overførselsgrundlag efter databeskyttelsesforordningens kapitel V. Ved en overførsel dokumenteres modtager, land, formål og grundlag samt, hvor påkrævet, vurdering af beskyttelsesniveauet og supplerende foranstaltninger. Fjernadgang for support, drift, udvikling og administration indgår i vurderingen. En udenlandsk myndigheds anmodning er ikke i sig selv kundens instruks eller et tilstrækkeligt grundlag for overførsel.

8 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. den registreredes indsigtsret
- d. retten til berigtigelse
- e. retten til sletning (»retten til at blive glemt«)
- f. retten til begrænsning af behandling
- g. underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
- h. retten til dataportabilitet
- i. retten til indsigelse
- j. retten til at gøre indsigelse mod resultatet af automatiske individuelle afgørelser, herunder profilering

2. Databehandleren bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, jf. art. 28, stk. 3, litra f.

Dette indebærer, at databehandleren under hensyntagen til behandlingens karakter skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

- a. forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen
- b. forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødigt forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet, medmindre det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.
- c. forpligtelsen til – uden unødigt forsinkelse – at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
- d. forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
- e. forpligtelsen til at høre tilsynsmyndigheden (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. Parternes eventuelle regulering/aftale om vederlæggelse eller lignende i forbindelse med databehandlerens bistand til den dataansvarlige vil fremgå af denne aftales bilag D.

9 Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en eventuel underdatabehandler. Databehandlerens første underretning skal ske uden unødigt forsinkelse og senest 72 timer efter, at databehandleren er blevet bekendt med bruddet. Fristen er en ydergrænse og berettiger ikke til at afvente underretning. Manglende fuldstændige oplysninger må ikke forsinke den første underretning.

2. I overensstemmelse med denne aftales afsnit 8, punkt 2, litra b, skal databehandleren - under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for denne - bistå den dataansvarlige med at foretage anmeldelse af bruddet til tilsynsmyndigheden. Det kan betyde, at databehandleren bl.a. skal hjælpe med at tilvejebringe nedenstående oplysninger, som efter databeskyttelsesforordningens artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse til tilsynsmyndigheden:

- 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. Sandsynlige konsekvenser af bruddet på persondatasikkerheden
- c. Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden, herunder hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

3. Underretningen indeholder desuden navn og kontaktoplysninger på en kontaktperson, hvor kunden kan få yderligere oplysninger. Oplysninger kan gives trinvis uden yderligere unødigt forsinkelse, hvis de ikke alle er tilgængelige samtidig. Databehandleren dokumenterer hændelsen og sine afhjælpende handlinger.

10 Sletning og tilbagelevering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling forpligtes databehandleren til, efter den dataansvarliges valg, at slette eller tilbagelevere alle personoplysninger til den dataansvarlige, samt at slette eksisterende kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.

2. Den praktiske tilbagelevering, sletning og lovpligtige opbevaring fremgår af bilag C.3. Udl levering til kunden eller overførsel til en ny udbyder ophæver ikke Danosofts egen lovbestemte opbevaringsforpligtelse. Oplysninger, som opbevares af denne grund, må kun anvendes til opbevaringen, nødvendig sikkerhed og lovlig udlevering.

11 Tilsyn og revision

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise databehandlerens overholdelse af databeskyttelsesforordningens artikel 28 og denne aftale, 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. Den nærmere procedure for den dataansvarliges tilsyn med databehandleren fremgår af denne aftales Bilag C.
3. Den dataansvarliges tilsyn med eventuelle underdatabehandlere sker som udgangspunkt gennem databehandleren. Den nærmere procedure herfor fremgår af denne aftales Bilag C.
4. Databehandleren er forpligtet til at give myndigheder, der efter den til enhver tid gældende lovgivning har adgang til den dataansvarliges og databehandlerens faciliteter, eller repræsentanter, der optræder på myndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

12 Parternes aftaler om andre forhold

1. En eventuel (særlig) regulering af konsekvenserne af parternes misligholdelse af databehandlersaftalen vil fremgå af parternes "hovedaftale" eller af denne aftales Bilag D.
2. En eventuel regulering af andre forhold mellem parterne vil fremgå af parternes "hovedaftale" eller af denne aftales Bilag D.
3. Hovedaftalens ansvarsbegrænsninger og vilkår om tredjepartsløsninger fritager ikke Danosoft for ufravigelige pligter efter databeskyttelses- eller bogføringsreglerne. De begrænser ikke registreredes rettigheder efter artikel 82 eller Danosofts forpligtelser for underdatabehandlere efter denne aftale.

13 Ikrafttræden og ophør

1. Denne aftale træder i kraft, når kunden accepterer den, eksempelvis ved at sætte flueben i Saldi. Kundens accept registreres med aftaleversion, tidspunkt og den bemyndigede repræsentant. Aftalen regulerer behandlingen mellem kunden og Danosoft fra den dokumenterede ikrafttræden og indebærer ikke i sig selv en tilbagevirkende overdragelse af tidligere aftaler med andre juridiske enheder.
2. Aftalen kan af begge parter kræves genforhandlet, hvis lovændringer eller u hensigtsmæssigheder i aftalen giver anledning hertil.
3. Parternes eventuelle regulering/aftale om vederlæggelse, betingelser eller lignende i forbindelse med ændringer af denne aftale vil fremgå af parternes "hovedaftale" eller af denne aftales bilag D.
4. Ophør af hovedaftalen medfører ophør af de almindelige behandlingstjenester, med forbehold for tilbagelevering, sletning og fortsat opbevaring efter afsnit 10 og bilag C.3. Databehandlersaftalen kan ikke opsiges særskilt i strid med afsnit 1, punkt 4, og afsnit 13, punkt 5.
5. Aftalen er gældende, så længe behandlingen består. Uanset "hovedaftalens" opsigelse, vil databehandlersaftalen forblive i kraft frem til behandlingens ophør og oplysningernes sletning hos databehandleren og eventuelle underdatabehandlere.
6. Danosoft kan ændre denne aftale med mindst én måneds skriftligt varsel til kunden, når ændringen er nødvendig på grund af ændret lovgivning eller myndighedspraksis, eller når ændringen ikke forringer beskyttelsen af kundens personoplysninger. Andre ændringer kræver kundens accept. Ændringer af underdatabehandlere følger bilag B. Den gældende version er tilgængelig på Danosofts hjemmeside, og tidligere versioner udleveres på anmodning.

Bilag A Oplysninger om behandlingen

A.1 Formål og karakter

Formålet er, at kunden kan anvende Saldi til bogføring, fakturering, kreditor-, lager-, ordre-, sags- og kundestyring samt de moduler, herunder eventuelt løn og POS, som er omfattet af kundens aftale. Behandlingen omfatter desuden automatisk aflæsning af bilag (OCR), jf. C.1.

Behandlingen består af modtagelse, registrering, strukturering, opbevaring, visning, søgning, ændring, eksport, sletning og aftalt overførsel samt drift, support, fejlfhjælpning, test af nye versioner af Saldi forud for udrulning, sikkerhedskopiering og genopretning. Supportadgang sker inden for kundens dokumenterede instruks og begrænses til det nødvendige.

A.2 Personoplysninger og registrerede

Oplysningerne omfatter navn, adresse, e-mail, telefon, kontooplysninger og personhenførbare virksomhedsoplysninger samt oplysninger om fakturaer, betalinger, transaktioner, ordrer og bilag. Brugernavne, roller og relevante logoplysninger behandles på kundens vegne i det omfang, formålet er kundens anvendelse og sikkerhed.

Registrerede er kundens nuværende og tidligere kunder, leverandører, medarbejdere, brugere, kontaktpersoner og øvrige personer i kundens dokumenter og registreringer. Ved lønbehandling kan CPR-numre, løn-, skatte-, ansættelses- og fraværsoplysninger indgå. Kunden skal have relevant behandlingsgrundlag, herunder for CPR-numre og eventuelle oplysninger efter artikel 9 eller 10. Særlige kategorier kan forekomme i eksempelvis fraværdata eller bilag og skal i så fald omfattes af den konkrete instruks og sikkerhedsvurdering.

Kunden begrænser indlæste oplysninger til det nødvendige. Saldi skal ikke anvendes til andre kategorier eller formål end de aftalte uden en ajourført instruks og vurdering af de nødvendige sikkerhedsforanstaltninger.

A.3 Varighed

Behandlingen på kundens vegne påbegyndes efter aftalens ikrafttræden og varer, så længe de aftalte tjenester leveres, samt under nødvendig tilbagelevering, sletning og lovpligtig opbevaring efter bilag C.3.

Bilag B Underdatabehandlere

B.1 Godkendelse og varsling

Kunden godkender ved aftalens indgåelse de underdatabehandlere, opgaver og behandlingslande, der fremgår af B.2. Kunden giver samtidig en generel skriftlig godkendelse til, at Danosoft kan tilføje eller udskifte underdatabehandlere efter nedenstående procedure.

Danosoft varsler skriftligt tilføjelser, udskiftninger og ændringer i opgaver eller behandlingssteder mindst én måned før planlagt ibrugtagning. Varslet oplyser juridisk navn, registreringsnummer, opgave, berørte oplysninger, steder og lande, planlagt dato og eventuelt overførselsgrundlag.

Kunden kan inden for varslingsperioden stille spørgsmål og gøre indsigelse, når der er rimelige og konkrete databeskyttelsesmæssige grunde hertil. Parterne søger i så fald at finde en løsning. Kan en løsning ikke findes, inden ændringen træder i kraft, kan kunden opsige de berørte tjenester med virkning fra ændringens ikrafttræden uden opsigelsesvarsel og uden gebyr. Allerede betalt vederlag refunderes ikke.

Den generelle godkendelse omfatter også leverandører i efterfølgende led, som en godkendt underdatabehandler anvender til den godkendte opgave, når de er pålagt tilsvarende databeskyttelsesforpligtelser. Behandling uden for EU/EØS er ikke omfattet af den generelle godkendelse og kræver særskilt instruks efter C.5.

B.2 Liste og opgaver

Underdatabehandler	Registreret adresse	Godkendt opgave og land
Kikkenborg Fiber & IT ApS CVR 34690510 Binavn: Kikkenborgs Dataservice ApS	Søndermarken 2 6670 Holsted Danmark	Hosting og serverdrift, herunder opbevaring og backup inden for instruksen. Danmark.
Opper Technology AB Org.nr. 559446-3720	Västerängsvägen 51 A 182 47 Enebyberg Sverige	Maskinlæringsbaseret aflæsning af bilag (OCR), jf. C.1. EU/EØS: platform i Sverige og modelleverandører inden for EU/EØS.

Godkendelsen omfatter de i bilag A beskrevne oplysninger og registrerede, alene i det omfang den enkelte leverandørs aftalte opgave nødvendiggør behandling. Leverandørerne må ikke anvende oplysningerne til egne formål. Den tilladte geografiske ramme, også for backup og support, følger ovenstående liste og C.4.

Opper Technology AB videresender forespørgsler til modelleverandører i efterfølgende led efter sin offentlige liste over underdatabehandlere på opper.ai/sub-processors. Danosoft anvender alene ruter, der behandler oplysningerne inden for EU/EØS uden dataopbevaring (zero data retention), og som ikke anvender oplysningerne til træning.

Kundens direkte aftale med en tredjepart, herunder kundens egne integrationer via API, giver ikke Danosoft en udvidet instruks, og tredjeparten er ikke Danosofts underdatabehandler.

Bilag C Instruks og sikkerhed

C.1 Behandling og AI

Databehandleren stiller Saldi til rådighed og behandler de i bilag A beskrevne oplysninger med henblik på de aftalte funktioner. Adgang gennem integrationer og API sker inden for kundens autorisation og instruks.

Kundens data, herunder personoplysninger, dokumenter, prompts, input og output, må ikke anvendes af Danosoft eller dets leverandører til træning, finjustering eller generel forbedring af egne eller fælles AI-modeller. Danosoft må heller ikke anonymisere eller aggregere kundedata til dette formål. Et forudafkrydset felt, manglende fravalg eller almindelig brug af Saldi giver ingen træningstilladelse. En senere ændring kræver en særskilt, udtrykkelig aftale samt dokumenteret vurdering af roller, behandlingsgrundlag, information til registrerede og deres rettigheder; kundens tilvalg er ikke i sig selv samtykke fra personer i kundens data. Samtaler med hjælpebotten følger dog reglerne nedenfor.

Ved træning forstås i denne aftale enhver anvendelse af data til at udvikle eller tilpasse en AI-model, herunder forudgående træning, finjustering og forstærkningslæring, samt opbygning af datasæt til disse formål.

Test og evaluering: Med kundens udtrykkelige accept kan Danosoft anvende kundens data til at teste og evaluere AI-modeller, eksempelvis til at sammenligne kvaliteten af OCR-aflæsning, med henblik på at vælge og kvalitetssikre de funktioner, der leveres til kunden. Accepten gives ved, at kundens administrator sætter flueben i Saldi, og Saldi registrerer, hvem der har accepteret, og hvornår. Accepten udgør kundens instruks og angiver, hvilke data testen omfatter. Testen sker inden for rammerne af B.2 og C.4 og omfatter ikke flere data end nødvendigt. Testdata og testresultater, der indeholder personoplysninger, slettes, når testen er afsluttet, og senest 30 kalenderdage efter testens start. Test efter dette afsnit er hverken træning eller generel forbedring af AI-modeller i ovenstående forstand. Et forudafkrydset felt, manglende fravalg eller almindelig brug af Saldi udgør ikke accept, og kunden kan til enhver tid trække sin accept tilbage.

Ved aftalens indgåelse omfatter instruksen følgende funktion, som anvender maskinlæring:

- OCR: maskinlæringsbaseret aflæsning af tekst og beløb fra bilag, som kunden uploader, med henblik på registrering i Saldi. Behandlingen sker hos Opper Technology AB inden for EU/EØS, jf. B.2. Bilag og aflæste data gemmes ikke hos leverandøren efter aflæsningen og anvendes ikke til træning eller forbedring af modeller.

Hjælpebot: Saldi indeholder en hjælpebot, der besvarer brugernes spørgsmål om anvendelse af Saldi. Hjælpebotten har ikke adgang til kundens regnskabsdata. Samtaler med hjælpebotten behandles af Danosoft som dataansvarlig efter Danosofts privatlivspolitik og ikke som databehandler efter denne aftale, jf. afsnit 1, punkt 13. Over for kunden forpligter Danosoft sig dog til følgende: Samtalerne opbevares i 6 måneder på en server hos Hostinger i Tyskland. Danosoft gennemgår spørgsmålene for at forbedre hjælpeetekster og vejledninger til Saldi. Brugere informeres herom i hjælpebotten og bør ikke indtaste personoplysninger om andre end sig selv.

Træning på samtaler med hjælpebotten: Samtaler med hjælpebotten må kun anvendes til træning eller finjustering af AI-modeller, jf. definitionen ovenfor, hvis kunden har givet udtrykkelig accept. Accepten gives ved, at kundens administrator sætter flueben i Saldi, og Saldi registrerer, hvem der har accepteret, og hvornår. Accepten omfatter alene samtaler fra kundens egne brugere. Et forudafkrydset felt, manglende fravalg eller almindelig brug af Saldi udgør ikke accept, og kunden kan til enhver tid trække sin accept tilbage med virkning for fremtidige samtaler. Træningen sker inden for EU/EØS, og samtalerne, herunder kopier i træningsdatasæt, slettes efter 6 måneder. Brugere informeres om træningen i hjælpebotten og kan gøre indsigelse efter Danosofts privatlivspolitik.

Andre AI-funktioner må først påbegyndes efter særskilt dokumenteret instruks, som angiver funktion, oplysninger, modtagere, behandlingslande, opbevaring og sikkerhedsforanstaltninger. En ekstern modelleverandør skal godkendes efter bilag B. Danosoft skal sikre, at leverandørvilkår og tekniske indstillinger overholder instruksen og forbuddet mod træning.

C.2 Behandlingssikkerhed

Sikkerhedsniveauet fastlægges efter afsnit 5 og en dokumenteret risikovurdering. Fravær af særlige kategorier af personoplysninger er ikke i sig selv grundlag for lavere sikkerhed. For de funktioner, som omfattes af kravene til registrerede digitale standard bogføringssystemer, skal Danosoft samtidig opfylde kravene til høj it-sikkerhed, herunder netværk, adgang, leverandører, backup, logning, beredskab, retablering og databeskyttelse.

Følgende foranstaltninger er aftalte minimumskrav:

- Brugeradgang og dataoverførsel beskyttes af krypterede forbindelser, herunder HTTPS med gyldigt certifikat.
- Brugeradgang kræver regnskabsnavn, brugernavn og adgangskode og anvender individuelle legitimationsoplysninger. Adgange begrænses efter arbejdsopgave, gennemgås regelmæssigt og fjernes straks, når autorisationen ophører. Administrator- og fjernadgang skal beskyttes med foranstaltninger, som imødegår de dokumenterede risici, herunder flerfaktoraутentifikation, hvor det er nødvendigt.
- API-adgang sker gennem HTTPS/JSON med korrekt regnskabsnavn, brugernavn og API-nøgle og kan begrænses til autoriserede IP-adresser. Systemadgang sker gennem SSH for autoriseret personale fra autoriserede IP-adresser. Rettigheder og nøgler begrænses og beskyttes efter det nødvendige adgangsbehov. Ændringer må ikke sænke det aftalte eller lovpligtige sikkerhedsniveau.
- Der gennemføres passende netværksbeskyttelse, vedligeholdelse og håndtering af sårbarheder. Sikkerhedsrelevante hændelser logges, og adgang til logdata begrænses.
- Danosoft styrer og fører risikobaseret tilsyn med underdatabehandlere. Hosting hos en leverandør flytter ikke Danosofts ansvar efter aftalen.
- Der gennemføres sikkerhedskopiering og mulighed for genopretning, og sikkerheden og gendannelsen afprøves regelmæssigt. Der tages daglig backup til to eksterne lokationer i overensstemmelse med den aftalte ydelse. Backup skal desuden opfylde § 7 i kravbekendtgørelsen, jf. C.3.3, herunder mindst ugentlig fuld og daglig inkrementel kopi samt opbevaring af mindst én sådan fuld og inkrementel kopi i EU/EØS.
- Lovpligtigt bevarede regnskabsdata opbevares beskyttet mod ændring og tab. Krypterede data kan dekrypteres, når lovlig udlevering er nødvendig. Opbevaret regnskabsbackup er krypteret.
- Der findes dokumenterede procedurer for sikkerhedsbrud, beredskab, retablering, sletning og bistand til kunden. Sporbarhed og håndtering af kundens lovlige sletteanmodninger understøttes.

C.3 Opbevaring, udlevering og sletning

C.3.1 Under abonnementet behandles oplysninger inden for kundens instruks og relevante opbevaringsfrister. Lovpligtigt regnskabsmateriale bevares i den periode, reglerne kræver. Øvrige oplysninger begrænses til det nødvendige for de aftalte formål.

C.3.2 Kunden kan inden ophør benytte de tilgængelige eksportfunktioner og kan i 30 kalenderdage efter ophør anmode om tilbagelevering. Udleveringen omfatter kundens data i et almindeligt anvendt, struktureret og maskinlæsbart format samt de tilhørende dokumenter og bilag i læsbart format. Udlevering sker sikkert til kunden eller dennes dokumenteret bemyndigede modtager. Fristen begrænser ikke lovpligtig opbevaring, GDPR-rettigheider eller ufravigelige rettigheder ved leverandørskifte. Ved leverandørskifte gælder også handelsbetingelsernes bestemmelser om leverandørskifte. En rettidigt bestilt udlevering afsluttes, før de omfattede data slettes.

C.3.3 Bogførte transaktioner og de bilag, som er omfattet af § 3 i bekendtgørelse nr. 97 af 26. januar 2023 om krav til digitale standard bogføringssystemer med senere ændringer (kravbekendtgørelsen), opbevares i fem år fra udgangen af det regnskabsår, materialet vedrører, jf. § 6 og bilag 1, punkt 4. Pligten gælder også efter ophør, konkurs, tvangsopløsning og flytning til en anden udbyder. Den lovpligtige opbevaring er ikke betinget af køb af arkivlicens og medfører ikke i sig selv fortsat abonnements- eller brugeradgang. Andre lovbestemte opbevaringskrav anvendes kun på det materiale og i den periode, de konkret omfatter.

C.3.4 Den almindelige brug af data ophører, når behandlingstjenesten ophører. Oplysninger, som fortsat skal opbevares ved lov, beskyttes mod uvedkommende adgang og begrænses til opbevaring, nødvendig sikring, genopretning og lovlig udlevering. Materialet skal kunne gendannes og gøres læsbart. Lovlige myndighedsanmodninger håndteres efter kravbekendtgørelsens §§ 10-11, herunder de deri fastsatte frister, betingelser og formater.

C.3.5 Oplysninger, som ikke skal bevares ved lov eller efter en fortsat lovlig og dokumenteret arkivinstruks, slettes fra aktive systemer uden unødigt forsinkelse efter kundens instruks, når tilbagelevering eller den relevante behandling er afsluttet. Ved manglende anden instruks påbegyndes sletningen ved udløbet af udleveringsvinduet og afsluttes senest 30 kalenderdage derefter. Hvis en rettidigt bestilt udlevering fortsat behandles, beregnes denne yderfrist fra dens afslutning. Lovpligtigt bevarede oplysninger slettes uden unødigt forsinkelse og senest 30 kalenderdage efter opbevaringspligtens udløb, medmindre et andet konkret lovkrav eller en fortsat lovlig instruks nødvendiggør opbevaring. Danosoft bekræfter sletningen skriftligt på anmodning og oplyser om eventuelle resterende lovligt bevarede kopier og deres slettefrist.

C.3.6 Femårsfristen omfatter alene det lovpligtige regnskabsmateriale. Øvrige oplysninger slettes også fra driftsbackup, hvor det er teknisk muligt. Kan oplysninger ikke slettes enkeltvis, skal kopien være utilgængelig for almindelig brug og udløbe ved en dokumenteret rotationscyklus senest 30 kalenderdage efter sletningen fra det aktive system. Ved gendannelse gentages tidligere sletninger, før oplysningerne bliver tilgængelige i drift. Lovpligtigt regnskabsmateriale og nødvendige sikkerhedskopier heraf bevares efter C.3.3 og C.3.4; øvrige oplysninger må ikke medtages i dette arkiv uden selvstændigt lovligt formål. Fristerne på 30 kalenderdage er aftalte yderfrister.

C.3.7 En særskilt arkivlicens beskriver den yderligere adgang eller service, kunden køber, hvilke oplysninger der behandles, og hvor længe. Kundens direkte adgang ophører ved arkivlicensens udløb; lovpligtig opbevaring og sletning følger fortsat C.3.3-C.3.6.

C.3.8 Log- og supportoplysninger begrænses til det, der er nødvendigt til det konkrete formål. Danosoft fastlægger, dokumenterer og anvender formålsbestemte slettefrister og oplyser dem til kunden på anmodning. Sådanne oplysninger slettes, når formålet ophører, medmindre en konkret sikkerhedshændelse eller lovbestemt pligt nødvendiggør afgrænset opbevaring. En dokumenteret undtagelse skal angive oplysninger, hjemmel, formål og ophørskriterium.

C.4 Behandlingssteder

Hosting, lagring og backup af kundens data sker hos Kikkenborg Fiber & IT ApS, Søndermarken 2, 6670 Holsted, Danmark, og må alene ske i Danmark. OCR behandles hos de underdatabehandlere og i de lande, der er anført i B.2.

Danosofts egen behandling og administrative adgang samt underdatabehandlernes drifts- og supportadgang må alene ske fra EU/EØS. Danosoft dokumenterer server- og backupplaceringer samt administrative adgangssteder og stiller oplysningerne til rådighed ved kundens kontrol efter afsnit 11. Ændringer i behandlingssteder eller leverandører følger B.1. Behandling fra lande uden for EU/EØS kræver desuden en særskilt instruks og opfyldelse af afsnit 7. Kundens egen fjernadgang giver ikke Danosoft eller leverandørerne en tilsvarende udvidet adgang.

C.5 Tredjelande

Hvis kunden ikke i dette bilag eller ved en senere dokumenteret instruks har godkendt en konkret tredjelandsoverførsel, er den ikke tilladt efter denne aftale, med forbehold for afsnit 7, punkt 1. En godkendt overførsel skal beskrive modtager, land, opgave, oplysninger, grundlag og nødvendige garantier. Alle behandlings- og fjernadgangslande registreres, også hvor adgang efter en konkret vurdering ikke udgør en overførsel til en særskilt modtager. Kapitel V anvendes, når dets betingelser er opfyldt.

C.6 Kundens tilsyn

Den dataansvarlige kan for egen regning indhente en revisionserklæring fra en uafhængig tredjepart angående databehandlerens overholdelse af denne databehandleraftale med tilhørende bilag.

Den dataansvarliges eventuelle udgifter i forbindelse med et fysisk tilsyn afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsagligt den tid), der er nødvendige for, at den dataansvarlige kan gennemføre sit tilsyn.

Revisions- og inspektionsmulighederne efter afsnit 11 består uanset, om Danosoft har en certificering eller revisionserklæring. Tilsyn planlægges med rimeligt varsel, medmindre en hændelse eller myndighedskrav nødvendiggør hurtigere tilsyn. Fortrolighed og hensynet til andre kunders oplysninger iagttages uden at hindre effektiv kontrol.

C.7 Tilsyn med underdatabehandlere

Databehandleren skal på foranledning af den dataansvarlige, for den dataansvarliges regning, indhente en revisionserklæring fra en uafhængig tredjepart angående underdatabehandlerens overholdelse af de forpligtelser, der er pålagt underdatabehandleren efter afsnit 6.

Databehandleren eller en repræsentant for databehandleren har herudover adgang til at føre tilsyn, herunder fysisk tilsyn, hos underdatabehandleren, når der efter databehandlerens (eller den dataansvarliges) vurdering opstår et behov herfor.

Kundens adgang til at kræve kontrol supplerer Danosofts løbende, risikobaserede leverandørkontrol. Opfyldelsen af Danosofts egne lovpligtige kontrolforpligtelser afhænger ikke af, at kunden bestiller en særskilt revision.

Bilag D Parternes øvrige forhold

D.1 Bistand og betaling

Hvis den dataansvarlige ønsker bistand til at besvare anmodninger om udøvelsen af de registreredes rettigheder efter databeskyttelsesforordningens kapitel III, yder databehandleren gratis bistand i 1 time. Bistand ud over den første time betales af den dataansvarlige.

Hvis den dataansvarlige anmoder om oplysninger eller bistand vedrørende sikkerhedsforanstaltninger, dokumentation eller databehandlerens behandling af personoplysninger generelt, og anmodningen går ud over, hvad der er nødvendigt efter gældende databeskyttelseslovgivning, kan databehandleren kræve betaling for den yderligere bistand.

Bistand i forbindelse med brud på persondatasikkerheden, som skyldes databehandleren eller dennes underdatabehandlere, ydes uden betaling.

Betaling aftales og opkræves i overensstemmelse med ufravigelige regler. En betalingsuenighed må ikke forsinke nødvendig håndtering af sikkerhedsbrud, lovpligtig udlevering eller anden tidskritisk bistand. Standarddokumentation, som er nødvendig efter artikel 28, stilles til rådighed efter afsnit 11.