Databehandleraftale for ServiceStep

Version 1.0 · gælder fra 2026-10-30

Hent som PDF

Denne aftale fastlægger IT Eksperten ApS' behandling af personoplysninger ved levering af ServiceStep på kundens vegne. Den omfatter hovedvilkår og bilag om instruks, underdatabehandlere, sikkerhed, sletning og kontakt.

1 Parter og roller

Kunden er den juridiske person, som indgår ServiceStep-abonnementet, identificeret i abonnements- eller ordreoplysningerne. Leverandøren er IT Eksperten ApS, CVR 35398929, Stenbjerg 10, 3200 Helsinge, info@servicestep.dk. Samme standardtekst og fælles bilag anvendes for alle kunder; der kræves ikke et særskilt udfyldt aftaledokument.

Når kunden bestemmer formål og væsentlige hjælpemidler, er kunden dataansvarlig og leverandøren databehandler. Hvis kunden selv behandler oplysninger på vegne af sine kunder, er kunden databehandler og leverandøren underdatabehandler. Kunden skal i det tilfælde dokumentere sin adgang til at give instruksen og til at anvende leverandøren og de relevante underdatabehandlere.

Aftalen supplerer service-/licensaftalen. Ved modstrid om persondatabehandling har denne aftale forrang. Hvis kunden selv er databehandler, er leverandøren underdatabehandler inden for kundens lovlige bemyndigelse. Kunden skal have den nødvendige tilladelse fra sine dataansvarlige; standardaftalen udvider ikke kundens instruktionsret.

2 Genstand formål og varighed

Behandlingen sker for at stille ServiceStep til rådighed til sagsbehandling, beskeder, kontakt- og opgavestyring, aftalte tidsfunktioner, dokumenthåndtering, drift og relevante integrationer. Oplysningstyper, registrerede, behandlinger og eventuelle begrænsninger fremgår af bilag A.

Aftalen gælder fra den dokumenterede ikrafttrædelse og indtil alle oplysninger omfattet af instruksen er tilbageleveret eller slettet efter bilag C og D. Fortrolighed og relevante bistandsforpligtelser fortsætter, så længe leverandøren lovligt besidder oplysninger.

3 Dokumenteret instruks

Leverandøren må kun behandle oplysninger efter kundens dokumenterede instruks, herunder ved overførsel til tredjelande. Instruksen består af denne standardaftale med fælles bilag, kundens lovlige konfiguration og dokumenterede bestillinger fra bemyndigede personer.

Leverandøren underretter kunden, hvis en instruks efter leverandørens opfattelse er i strid med databeskyttelsesreglerne. Den berørte behandling sættes på pause, indtil forholdet er afklaret, når dette kan ske uden at tilsidesætte ufravigelige forpligtelser.

Hvis EU-ret eller national ret, som leverandøren er underlagt, kræver anden behandling, orienteres kunden før behandlingen, medmindre loven forbyder det. Leverandøren bruger ikke kundedata til egne nye formål eller til generel modeltræning under denne instruks.

4 Kundens forpligtelser

Kunden fastlægger et lovligt behandlingsgrundlag, opfylder sin oplysningspligt og indsamler kun nødvendige oplysninger. Kunden er ansvarlig for sine administratorers instrukser, brugerrettigheder, modtagervalg og aftaler med egne integrationsleverandører.

Kunden skal oplyse særlige risici og krav, føre en dokumenteret vurdering af leverandøren og fastlægge sletteinstrukser. Hvis formål eller datakategorier udvides væsentligt, skal parterne inden ændringen vurdere behov for at opdatere denne aftale og sikkerhedsforanstaltningerne.

5 Fortrolighed og adgang

Leverandøren sikrer, at personer med adgang er underlagt fortrolighed og kun får nødvendig adgang til arbejdsopgaven. Rettigheder tildeles, revurderes og tilbagekaldes efter en dokumenteret proces.

Medarbejderes supportadgang til kundens sagsdata kræver organisationsadministratorens godkendelse, er tidsbegrænset til den konkrete supportsag og registreres i en adgangslog. Organisationsadministratoren kan trække adgangen tilbage når som helst. Godkendelsen er en instruks og adgangstilladelse, ikke et generelt GDPR-samtykke fra de registrerede.

En platformadministratorrolle giver ikke i sig selv ret til fri brug af sagsindhold. Denne standardaftale indeholder ikke en generel undtagelse fra kravet om godkendelse af supportadgang. Nødvendig teknisk drift og sikkerhedsbehandling skal fortsat ske inden for den dokumenterede instruks og gældende ret.

6 Behandlingssikkerhed

Leverandøren gennemfører passende tekniske og organisatoriske foranstaltninger efter artikel 32 under hensyn til behandlingens karakter, omfang, kontekst, formål og risici. Foranstaltningerne konkretiseres i bilag C og skal kunne dokumenteres.

Foranstaltningerne skal bl.a. omfatte adgangsbeskyttelse, adskillelse af kunders oplysninger, beskyttelse under transmission og lagring, løbende fortrolighed og integritet, relevant tilgængelighed, evne til rettidig gendannelse og regelmæssig vurdering af effekten.

Ændringer må ikke reducere det aftalte sikkerhedsniveau væsentligt. Ændringer med betydning for kundens risiko eller instruks meddeles relevant. Teknisk funktionalitet eller en cloudleverandørs certificering er ikke alene dokumentation for den samlede installations sikkerhed.

7 Underdatabehandlere

Kunden giver generel skriftlig godkendelse til de underdatabehandlere, der er identificeret med opgave og behandlingssteder i det godkendte fælles bilag B. En leverandør, der alene er nævnt som en mulig integration, er ikke derved godkendt. Det endelige bilag skal være tilstrækkeligt udfyldt, før aftalen tages i brug.

Ved tilføjelse eller udskiftning varsles alle kundens organisationsadministratorer mindst 30 kalenderdage før ændringen. Varslet angiver leverandør, opgave, behandlingssted og relevante overførselsforhold. Kunden kan gøre

begrundet indsigelse inden ændringen.

Parterne søger en egnet løsning ved en begrundet indsigelse. Den omtvistede nye behandling sættes ikke i gang for kunden, mens forholdet er uafklaret. Kan leverandøren ikke tilbyde et alternativ, kan kunden opsige med virkning før ændringen og få den ubrugte del af et forudbetalt abonnement tilbage. Udlevering og sikker afvikling koordineres med ophøret.

Leverandøren pålægger hver underdatabehandler mindst de samme relevante databeskyttelsesforpligtelser ved en bindende aftale og forbliver ansvarlig over for kunden for underdatabehandlerens opfyldelse. Bilag B holdes ajour og kan udleveres til kunden.

8 Behandlingssteder og tredjelande

Applikation, database og ServiceSteps backup er oplyst placeret i Microsoft Azure Denmark East i Danmark. Platformens Microsoft 365 Exchange Online-mail har oplyst dataplacering i Nederlandene. Kundens eget fillager er ikke en del af denne placeringsangivelse. Placering af øvrige replikaer og relevant fjernadgang skal fremgå af den dokumenterede leverandør- og driftsopsætning.

Microsoft-aftalegrundlaget for den oplyste danske CSP-partnerkanal er Microsoft Customer Agreement med Microsoft Ireland Operations Limited som Microsoft-aftalepart. Microsofts DPA indgår ved henvisning. Den senest gennemgåede danske udgave er opdateret 22. maj 2026; den gældende udgave for et konkret abonnement følger dets aftale- og fornyelsesvilkår.

Overførsel til et tredjeland, herunder fjernadgang der udgør en overførsel, kræver dokumenteret instruks og et gyldigt grundlag efter GDPR kapitel V. Microsofts DPA beskriver standardkontraktbestemmelser mellem Microsoft Ireland Operations Limited og Microsoft Corporation samt supplerende foranstaltninger. Et europæisk datacenter erstatter ikke vurdering af den faktiske behandling og relevante produktvilkår.

Relevante parter, moduler, bilag, overførselsvurderinger og nødvendige supplerende foranstaltninger dokumenteres for de anvendte tjenester. Denne artikel 28-aftale er ikke i sig selv et overførselsgrundlag. Leverandøren orienterer om relevante myndighedsanmodninger, når det er tilladt, og begrænser udlevering til det lovligt nødvendige. Væsentlige ændringer i det anvendte overførselsgrundlag meddeles kunden.

9 Bistand ved registreredes rettigheder

Leverandøren bistår kunden med passende foranstaltninger ved anmodninger om indsigt, rettelse, sletning, begrænsning, indsigelse og dataportabilitet. Leverandøren besvarer ikke en sådan anmodning om kundens data selvstændigt uden instruks, medmindre loven kræver det.

Modtager leverandøren en anmodning, videresendes den uden unødig forsinkelse til kundens bemyndigede kontakt. Bistandens form, sikre overførsel og nødvendige frister aftales ud fra kundens lovpligtige svarfrist. Bistand må ikke forsinkes af en uafklaret særskilt betalingsdrøftelse, hvis dette vil forhindre lovlig håndtering.

10 Bistand ved risikovurdering og tilsyn

Leverandøren bistår kunden med oplysninger, som er nødvendige for at opfylde forpligtelserne efter artikel 32–36, herunder konsekvensanalyser, vurdering af sikkerhed, høring af tilsynsmyndighed og dokumentation af hændelser, under hensyn til behandlingens karakter og leverandørens oplysninger.

Rimeligt ekstraarbejde kan prissættes efter forudgående aftale, når det er lovligt og ikke vedrører afhjælpning af leverandørens egen misligholdelse. Betalingsvilkår må ikke gøre en lovpligtig bistand illusorisk.

11 Brud på persondatasikkerheden

Leverandøren underretter kunden uden unødig forsinkelse efter at være blevet bekendt med et brud på persondatasikkerheden vedrørende kundens data. En første underretning må ikke afvente en fuldstændig undersøgelse. Fristen for kundens eventuelle myndighedsanmeldelse må ikke forveksles med leverandørens underretningspligt.

Underretningen beskriver så vidt muligt hændelsen, berørte kategorier og omtrentligt antal registrerede og dataposter, kontaktpunkt, sandsynlige konsekvenser og iværksatte eller foreslåede afhjælpende foranstaltninger. Manglende oplysninger suppleres løbende.

Leverandøren begrænser skaden, bevarer relevant bevismateriale og bistår kunden med vurdering og eventuel underretning af myndighed og registrerede. Kommunikation skal ske via de sikre kontaktkanaler i bilag D, og hændelsen og beslutningerne dokumenteres. Kunden eller den relevante dataansvarlige træffer beslutning om anmeldelse, medmindre andet følger af lov.

12 Dokumentation revision og kontrol

Leverandøren stiller de oplysninger til rådighed, som er nødvendige for at påvise overholdelse af artikel 28 og denne aftale, og muliggør og bidrager til revisioner og inspektioner udført af kunden eller en af denne bemyndiget revisor.

Kontrol planlægges normalt med rimeligt varsel og mindst mulig påvirkning af drift og andre kunders oplysninger. Relevante rapporter kan bruges som første dokumentation, men kan ikke afskære yderligere nødvendig kontrol. Hændelser, konkret mistanke eller myndighedskrav kan kræve hurtigere eller udvidet kontrol.

Revision hos en cloud-underdatabehandler tilrettelægges efter dennes relevante aftalevilkår, suppleret med de nødvendige oplysninger og rettigheder. Dette fritager ikke leverandøren for at sikre kundens mulighed for reelt tilsyn eller fra eget ansvar. Rimelige praktiske aftaler om fortrolighed må ikke blokere lovpligtig kontrol.

13 Tilbagelevering og sletning

Under aktivt abonnement fastsætter kunden fristen for afsluttede sager og ToDo. Standard er 5 år fra seneste lukningsdato for sagen eller afslutningsdato for ToDo. Genåbning med senere ny lukning eller afslutning starter fristen forfra. Kunden skal vælge en periode, der passer til sit lovlige formål; standarden er ikke en generel lovpligtig opbevaringsfrist.

Ved abonnementsophør stilles kundens data til rådighed for organisationsadministratorens læsning og eksport i 30 dage fra den faktiske ophørsdato. Oprettelse og ændringer er låst. Den første samlede dataudlevering er inkluderet uden særskilt betaling. På kundens dokumenterede lovlige instruks tilbageleveres eller slettes oplysningerne, og leverandøren sletter eksisterende kopier efter den aftalte proces, medmindre EU-ret eller national ret kræver opbevaring.

Efter udleveringsperioden slettes kundedata fra den aktive løsning. Backupkopier udløber højst 30 dage efter den aktive sletning, normalt senest 60 dage efter ophør. I restperioden anvendes backup kun til nødvendig sikkerhed og lovlig gendannelse. Sletteinstrukser genanvendes ved gendannelse, før normal behandling fortsætter, hvor det er nødvendigt for at respektere instruksen.

Kundens eksternt lagrede filer slettes ikke ved sletning af sagen eller abonnementets data i ServiceStep. ServiceStep fjerner sine links og filoplysninger; kunden håndterer selve filerne og deres backup på egen storageplatform. Leverandørens egne eventuelle midlertidige kopier er fortsat omfattet af instruksen og skal begrænses og slettes efter det relevante formål.

Leverandøren dokumenterer gennemført sletning eller tilbagelevering, afgrænser eventuelle lovlige undtagelser og sikrer tilsvarende håndtering hos sine underdatabehandlere. Ufravigelige rettigheder, herunder relevante Data Act-krav ved leverandørskifte, må ikke afskæres af automatiske slettefrister eller en betalingsbetinget appspærring. Udlevering kan om nødvendigt håndteres uden for appen via info@servicestep.dk.

14 Aftalens indgåelse og dokumentation

Denne fælles standarddatabehandleraftale med fælles bilag indgår i abonnementsvilkårene for alle kunder. Ved abonnementsoprettelsen accepterer en bemyndiget organisationsadministrator licensvilkårene og denne aftale. Der udfærdiges ikke individuelle databehandleraftaler eller særskilte underskriftsdokumenter.

Kundens juridiske identitet fremgår af abonnementsoplysningerne. Person, tidspunkt og de accepterede dokumentversioner registreres og kan dokumenteres. Offentliggørelse på loginsiden eller almindeligt brugerlogin er ikke i sig selv accept på organisationens vegne. Aftalen ændrer ikke registreredes rettigheder efter gældende ret.

Bilag A Fælles behandlingsinstruks

Dette bilag gælder alle kunder. Den konkrete behandling afgrænses af kundens abonnement, aktiverede moduler, lovlige konfiguration og dokumenterede instrukser. Kunden er dataansvarlig for egne formål eller databehandler med fornøden bemyndigelse fra sine dataansvarlige.

Formålet er levering af sags- og opgavestyring, beskeder, kontakter, kalender, aftalte tidsfunktioner, rapportering, filhåndtering gennem kundens lager og relevante integrationer samt nødvendig drift, sikkerhed, support, udlevering og sletning. Varigheden følger abonnementet og den efterfølgende udleverings- og sletteproces.

De registrerede er kundens autoriserede medarbejdere, kontaktpersoner, kunder, leverandørkontakter og andre personer, som lovligt indgår i kundens sager og opgaver. Oplysninger kan omfatte identitet og kontakt, rolle og organisation, sags- og beskedindhold, interne noter, opgaver, kalender, aktive arbejdsperioder og godkendt tid, filmetadata, filindhold under håndtering samt nødvendige login- og hændelsesoplysninger.

Behandlingen omfatter indsamling, registrering, organisering, opbevaring, søgning, visning, rettelse, kommunikation til aftalte modtagere, rapportering, sikkerhedskopiering, udlevering og sletning. Filindhold kan passere gennem ServiceStep ved upload, download og relevante sikkerhedsfunktioner; permanent filopbevaring sker på kundens tilsluttede storageplatform.

Artikel 9-oplysninger, CPR-numre og oplysninger om strafbare forhold efter artikel 10 er ikke del af standardinstruksen. Sådan brug kræver særskilt aftale, lovligt grundlag og sikkerhedsvurdering. Utilsigtet modtagelse håndteres efter instruks og relevante sikkerhedsprocedurer.

Kundens aktivering af en integration er kun instruks til den konkrete funktion inden for dens tilladelser. En generel liste over mulige integrationer er ikke et blanketmandat til nye modtagere eller nye behandlingsformål. Rolle, leverandør, dataflow og tilladelser skal være dokumenteret for den faktisk aktiverede funktion.

Bilag B Driftsleverandører og aftalekæde

Microsoft Ireland Operations Limited er den Microsoft-aftalepart, der fremgår af Microsofts officielle kundeaftale for Danmark, dansk, CSP Partner og Commercial. Aftalen indarbejder Microsofts DPA ved henvisning. Azure og Microsoft 365 er tjenester under dette aftalegrundlag; den relevante underleverandørkæde og faktiske behandling følger de anvendte tjenester og produktvilkår.

Microsoft Corporation er særskilt omtalt som part i DPA'ens standardkontraktbestemmelser om internationale overførsler. Dette må ikke forveksles med den danske kundeaftales Microsoft-aftalepart. Den aktuelle underdatabehandlerliste og relevante behandlingssteder skal dokumenteres og holdes ajour for de faktisk anvendte tjenester.

Leverandør og tjeneste	Opgave	Oplyst dataplacering
Microsoft Ireland Operations Limited — Microsoft Azure	Hosting af applikation og database, backup samt teknisk overvågning.	Denmark East, Danmark, for applikation, database og backup. Øvrige relevante behandlingssteder skal dokumenteres.
Microsoft Ireland Operations Limited — Microsoft 365 Exchange Online	Platformens hovedmail og nødvendig mailkommunikation.	Nederlandene (Holland), oplyst af leverandøren. Øvrige relevante behandlingssteder skal dokumenteres.

Distributør og kundens egne udbydere

Cloud Factory ApS leverer abonnementer og fakturering for Azure og Microsoft 365. Der er efter leverandørens oplysninger ingen administrator- eller supportadgang til miljøerne, og Cloud Factory opføres derfor ikke alene på dette grundlag som underdatabehandler af kundernes sagsdata. Eventuelle egne bestillings- og faktureringsoplysninger vedrører et særskilt forhold.

Der anvendes efter leverandørens oplysninger ingen ekstern teknisk supportleverandør. Kundens egne storage-, mail- og øvrige integrationsudbydere har den rolle, som følger af den faktiske aftale og behandling. Kundens storageudbyder er ikke automatisk IT Ekspertens underdatabehandler. Microsofts DPA erstatter ikke denne aftale mellem IT Eksperten ApS og kunden.

Bilag C Sikkerhed og drift

Leverandøren anvender passende tekniske og organisatoriske foranstaltninger efter GDPR artikel 32. Den faktiske opsætning og dens effektivitet skal kunne dokumenteres. Denne beskrivelse udgør ikke en sikkerhedscertificering eller en uafhængig driftsrevision.

Adgang skal være personlig, arbejdsbetinget og afgrænset efter rolle og organisation. Påkrævet flerfaktorbeskyttelse anvendes, og adgangsrettigheder administreres og tilbagekaldes efter behov. Supportadgang følger den godkendelses-, tidsbegrænsnings- og logproces, der er beskrevet i hovedvilkårene.

Data skal beskyttes mod uautoriseret adgang, ændring, tab og videregivelse. Adgangshemmeligheder beskyttes, og transmission, filhåndtering og relevante sikkerhedsfunktioner indgår i risikovurderingen.

Overvågning sker i Azure. Leverandøren skal have processer for relevante opdateringer, fejl, sikkerhedshændelser og dokumentation af kontroller. Tekniske adgangs- og sikkerhedslogs opbevares i 90 dage. Sagshistorik følger sin egen frist. Nødvendigt materiale om en konkret hændelse kan undtagelsesvis bevares særskilt på dokumenteret grundlag.

Databasen sikkerhedskopieres dagligt. ServiceSteps backup opbevares i Denmark East og udløber senest efter 30 dage. Gendannelse fra backup testes hver tredje måned i testmiljøet, og gennemførelse og resultat dokumenteres. Der er ikke aftalt en bestemt gendannelsestid eller et garanteret maksimalt datatab.

Til login