Databehandler aftale FutureLink 2025

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

Mellem

[NAVN] CVR [CVR -NR]

[ADRESSE]

[POSTNUMMER OG BY]

[LAND]

herefter ”den dataansvarlige”

og

FutureLink ApS

CVR 45 88 40 90

herefter ”databehandleren” der hver især er en ”part” og sammen udgør ”parterne”

HAR AFTALT følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder Databehandleraftale – & FutureLink ApS.

2. Præambel

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

2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa -Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).

3. I forbindelse med leveringen af BatchFlow -suiten behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

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

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

6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.

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

8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

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

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

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

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes1 nationale ret og disse Bestemmelser.

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger. 1 Henvisninger til "medlemsstat" i disse bestemmelse skal forstås som en henvisning til "EØS medlemsstater".

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

4. Databehandleren handler efter instruks

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

2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU -ret eller medlemsstaternes nationale ret.

5. Fortrolighed

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

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

6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici. Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

a. Pseudonymisering og kryptering af personoplysninger

b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.

d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

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

3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

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

7. Anvendelse af underdatabehandlere

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

2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående på forhånd at have adviseret den dataansvarlige. Databehandleren vil i praksis advisere dette, når der logges på BatchFlow -platformen, hvor brugeren vil blive mødt med en notifikation.

3. 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 underdat abehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

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

4. 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.

5. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige k an indtræde i Databehandleraftale – & FutureLink ApS – September 2025 Side 7 / 15 databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

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

8. Overførsel til tredjelande eller internationale organisationer

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

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

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

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

b. overlade behandling af personoplysninger til en underdatabehandler i et tredje land

c. behandle personoplysningerne i et tredjeland

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

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

9. Bistand til den dataansvarlige

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

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

a. oplysningspligten ved indsamling af personoplysninger hos den registrerede

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

c. indsigtsretten d. retten til berigtigelse

e. retten til sletning (”retten til at blive glemt”)

f. retten til begrænsning af behandling

g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling

h. retten til dataportabilitet

i. retten til indsigelse

j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Be stemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

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

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

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

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

3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10. Underretning om brud på persondatasikkerheden

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

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

3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kateg orierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger .

4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til a t slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er slettet.

12. Revision, herunder inspektion

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

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

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

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse a ndre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

14. Ikrafttræden og ophør

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

2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

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

5. Underskrift På vegne af den dataansvarlige

Navn [NAVN]

Stilling [STILLING]

Telefonnummer [TELEFONNUMMER]

E-mail [E-MAIL]

Underskrift På vegne af databehandleren

Navn Rune Juul

Stilling CEO

E-mail rju@futurelink.dk

Underskrift

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

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

Navn [NAVN]

Stilling [STILLING]

Telefonnummer [TELEFONNUMMER]

E-mail [E-MAIL] Navn Rune Juul

Stilling CEO

E-mail rju@futurelink.dk

Bilag A Oplysninger om behandlingen

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

Formålet med behandlingen er at levere BatchFlow-ydelsen . Ydelsen afhænger af, om løsningen er On-premise (hostes af kunden selv) eller Cloud (hostes af FutureLink).

Cloud inkluderer hosting og drift af systemet hos FutureLinks hostingpartner samt løbende opdateringer.

Ved on-premise står kunden selv for hosting og drift af systemer, og support til dette afregnes efter forbrugt tid. Løbende opdateringer er tilgængelige, og opdateringer af systemet foretages af FutureLink og afregnes efter forbrugt tid.

Ved begge løsninger afregnes generel support iht. FutureLinks Supportbetingelser. (Disse kan findes på vores hjemmeside)

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

At databehandleren ved anvendelse af sine IT -systemer behandler, herunder opbevarer, personoplysninger om den dataansvarliges kunder

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

Alle typer af personoplysninger, der behandles, er i kategorien almindelige personoplysninger (ikke-følsomme). Almindelige kontaktoplysninger på de personer, der er kontakter hos den Dataansvarlige Registrering af brugere af systemet med: navn, telefonnummer, e-mail samt brugerniveau: fx dem o, godkender, bogholder, administrator.

Brugernes eventuelle indtastede personoplysninger ved brug af BatchFlow-suiten (dette ser og tilgår Databehandleren ikke, medmindre Databehandleren på den Dataansvarliges opfordring bistår med fejlretning og support på specifikke data).

A.4. Behandlingen omfatter følgende kategorier af registrerede

Kunder og deres slutbrugere

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

Behandling følger det kontraktlige kundeforhold

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
xxx	xxx	xxx	xxx

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

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

Databehandleren må behandle Personoplysningerne med henblik på levering af BatchFlow-ydelsen

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle: Behandlingen omfatter en mindre mængde almindelige personoplysningen, hvorefter der skal etableres et mellem sikkerhedsniveau Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etableret det nødvendige (og aftalte) sikkerhedsniveau.

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

• Al kommunikation fra slutkunder til FutureLinks servere foregår krypteret via SSL/TLS

• Alle servere og arbejdsstationer er beskyttet af firewalls. Adgang til administration af servere er styret således, at det kun er godkendt personale fra godkendte fysiske placeringer, der kan tilgå serverne

• API-adgang sikres med et unikt serienummer pr. kunde

• Der benyttes endpoint protection på alle servere og på alle arbejdsstationer, der tilgår serverne

• Serverne og arbejdsstationer patches regelmæssigt med sikkerhedsopdateringer

• Der skal være ”revisionsspor”, så alle aktiviteter vedr. behandling af fakturaer logges

• Der skal være etableret en proces til change management og opgave håndtering

• Der skal være etableret en proces, der beskriver, hvordan ændringer implementeres fra test til driftssystemer

• Der skal være en proces for håndtering af onboarding og offboarding af medarbejdere, der har adgang til serverne

• Alle password gemmes krypteret

• Der skal være mulighed for 2-trinsgodkendelse for slutbrugere af BatchFlow

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for det nedenstående om fang og udstrækning – bistå den dataansvar-lige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

• Al kommunikation fra slutkunder til FutureLinks servere foregår krypteret via SSL/TLS

• Alle servere og arbejdsstationer er beskyttet af firewalls. Adgang til administration af servere er styret således, at det kun er godkendt personale fra godkendte fysiske placeringer, der kan tilgå serverne

• API-adgang sikres med et unikt serienummer pr. kunde

• Der benyttes endpoint protection på alle servere og på alle arbejdsstationer, der tilgår serverne

• Serverne og arbejdsstationer patches regelmæssigt med sikkerhedsopdateringer

• Der skal være "revisionsspor", så alle aktiviteter vedr. behandling af fakturaer logges

• Der skal være etableret en proces til change management og opgavehåndtering

• Der skal være etableret en proces, der beskriver, hvordan ændringer implementeres fra test til driftssystemer

• Der skal være en proces for håndtering af onboarding og off boarding af medarbejdere, der har adgang til serverne

• Alle password gemmes krypteret

• Der skal være mulighed for 2-trinsgodkendelse for slutbrugere af BatchFlow

• Der er installeret antivirus på enheder, hvorfra der kan tilgås personoplysninger

• Medarbejdere med adgang til personoplysninger modtager oplæring og passende awareness-træning

C.4 Opbevaringsperiode/sletterutine

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

C.5 Lokalitet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

FutureLink ApS

Njalsgade 21 F 2

2300 København S

FutureLink ApS medarbejderes hjemmearbejdsplads

Databehandleren har fastlagt retningslinjer for medarbejdernes behandling af personoplysninger ved anvendelse af hjemmearbejdspladser

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

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

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

Den dataansvarlige eller en repræsentant for den dataansvarlige foretager hvert andet år en fysisk inspektion af lokaliteterne, hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen, med henblik på at fastslå databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Ud over det planlagte tilsyn, kan den dataansvarlige gennemføre en inspektion hos databehandleren, når den dataansvarlige finder det nødvendigt.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion.

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

Databehandleren skal årligt for egen regning indhente en revisionserklæring/inspektionsrapport fra en uafhængig tredjepart vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af REVISIONSERKLÆRINGER/INSPEKTIONSRAPPORTER kan anvende s i overensstemmelse med disse bestemmelser:

ISAE 3000, ISAE 3402, ISRS 4400 eller tilsvarende

Rapporten vil være tilgængelige på databehandlerens hjemmeside, hvor de årligt opdateres med den nyeste indhentede version. Den dataansvarlige kan anfægte rammerne for og/eller metoden i rapporten og kan i sådanne tilfælde anmode om en ny rapport under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af rapporten, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU -ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Eller

Databehandleren eller en repræsentant for databehandleren foretager årligt en inspektion af underdatabehandleren, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen, med henblik på at fastslå underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Dokumentation for sådanne inspektioner fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af tilsynet, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU -ret eller medlemsstaternes nationale ret og disse Bestemmelser.

D. Retningslinjer for hjemarbejdsplads

Retningslinjer for hjemmearbejdsplads

FutureLink ApS
CVR: 45 88 40 90

Formål

Formålet med disse retningslinjer er at sikre, at behandling af personoplysninger ved hjemmearbejde sker i overensstemmelse med databeskyttelsesforordningen (GDPR), databehandleraftaler og FutureLinks interne politikker.

---

1. Fysisk sikkerhed

- Arbejdspladsen i hjemmet skal være afgrænset fra private omgivelser.
- Computer, mobil og dokumenter må ikke være tilgængelige for familie, gæster eller andre uvedkommende.
- Papirer og fysiske medier med personoplysninger skal opbevares aflåst, når de ikke bruges.

---

2. IT-udstyr

- Kun virksomhedens udstyr må bruges til behandling af personoplysninger.
- Udstyret skal altid være beskyttet med adgangskode, kryptering og seneste sikkerhedsopdateringer.
- Automatisk lås af skærm skal aktiveres (maks. 5 minutters inaktivitet).
- USB-nøgler eller eksterne harddiske må kun anvendes, hvis de er godkendt og krypterede.

---

3. Netværkssikkerhed

- Hjemmearbejdspladsen skal anvende et Wi-Fi med stærk adgangskode.
- Offentlige netværk må ikke anvendes uden VPN.

- Alle forbindelser til virksomhedens systemer skal ske via sikre, krypterede løsninger (VPN, SSL/TLS).

---

4. Behandling af data

- Udskrivning af dokumenter med personoplysninger skal begrænses mest muligt.
- Udskrevne dokumenter skal opbevares aflåst og bortskaffes sikkert (makulering).
- Personoplysninger må ikke gemmes lokalt på pc'en – kun på godkendte, sikrede

  servere/cloud-løsninger.

---

5. Fortrolighed

- Samtaler om personoplysninger må ikke ske, hvor uvedkommende kan lytte med.
- Skærme skal placeres, så de ikke kan ses af uvedkommende.
- Brug headset ved onlinemøder, hvor personoplysninger kan drøftes.

---

6. Hændelser

- Mistanke om brud på datasikkerheden (fx bortkomst af udstyr, indbrud, hacking) skal straks meldes til nærmeste leder og til FutureLinks databeskyttelsesansvarlige:
  rju@futurelink.dk.

---

7. Revision og kontrol

- Medarbejdere kan blive bedt om at bekræfte skriftligt, at de overholder disse retningslinjer.
- Der kan foretages stikprøver eller gennemføres tilsyn efter behov.

---

8. Ikrafttræden

Retningslinjerne træder i kraft den **01.10.2025** og gælder for alle medarbejdere i FutureLink, der arbejder helt eller delvist fra hjemmearbejdsplads.

Medarbejdererklæring

Retningslinjer for hjemmearbejdsplads
FutureLink ApS – CVR 45 88 40 90

Jeg bekræfter hermed, at jeg har modtaget og læst dokumentet **"Retningslinjer for hjemmearbejdsplads"**, og at jeg forstår og accepterer de krav og regler, der gælder for behandling af personoplysninger, når jeg arbejder hjemmefra.

Jeg er særligt opmærksom på følgende:

- Jeg må kun bruge virksomhedens udstyr til behandling af personoplysninger.
- Jeg skal beskytte adgang til udstyr og data med stærke passwords og følge virksomhedens sikkerhedskrav.
- Jeg må ikke lade uvedkommende få adgang til virksomhedens udstyr eller oplysninger.
- Jeg skal straks rapportere mistanke om brud på datasikkerheden til min leder og til FutureLinks databeskyttelsesansvarlige.
- Jeg er ansvarlig for at følge alle retningslinjer for fysisk sikkerhed, netværkssikkerhed og fortrolighed beskrevet i dokumentet.

Jeg er indforstået med, at overtrædelse af disse retningslinjer kan betragtes som misligholdelse af mine ansættelsesforpligtelser.

Medarbejder

Navn: _____

Stilling: _____

Dato: _____

Underskrift: _____