Databehandleraftale

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

Offentliggjort og gældende på: https://firma360.dk/dba/

Aftalen accepteres ved indgåelsen af en Hovedaftale med Firma360 ApS og finder automatisk anvendelse i hele Hovedaftalens løbetid uden krav om særskilt underskrift, medmindre parterne skriftligt aftaler andet.

DATABEHANDLER

Firma360 ApS
CVR-nr.: 39493691
Vandtårnsvej 106B, 2860 Søborg
E-mail: dba@firma360.dk
Web: firma360.dk

herefter benævnt "databehandleren"

DATAANSVARLIG

Den virksomhed eller person, som har indgået en Hovedaftale med Firma360 ApS. Den dataansvarliges identitet, kontaktperson og kontaktoplysninger fremgår af Hovedaftalen.

herefter benævnt "den dataansvarlige"

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.

1 Indhold

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. Nærværende Aftale er Firma360 ApS' standarddatabehandleraftale, offentliggjort på https://firma360.dk/dba/. I forbindelse med leveringen af webhosting, webudvikling, appudvikling, marketing/annoncering og konsulentydelser som nærmere beskrevet i aftalen mellem parterne ("Hovedaftalen"), behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser. Databehandleren behandler udelukkende personoplysninger på vegne af den dataansvarlige og ikke til egne formål, medmindre andet følger af EU-ret eller national ret.
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. Listen opdateres løbende på https://firma360.dk/dba/.
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 er omfattet af Bestemmelserne.
10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter. Den til enhver tid gældende version er tilgængelig på https://firma360.dk/dba/.
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 medlemsstaternes 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.
3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.
4. Den dataansvarlige bekræfter ved indgåelse af disse Bestemmelser, at:
   a) den dataansvarlige udelukkende behandler personoplysninger i overensstemmelse med kravene i den gældende databeskyttelseslovgivning;
   b) den dataansvarlige har et lovligt grundlag for at behandle og videregive personoplysninger til databehandleren, herunder til underdatabehandlere som databehandleren anvender;
   c) den dataansvarlige har ansvaret for nøjagtigheden, integriteten, indholdet, pålideligheden og lovligheden af de personoplysninger, som behandles af databehandleren;
   d) den dataansvarlige har opfyldt sine oplysningsforpligtelser over for de registrerede; og

e) den dataansvarlige er enig i, at databehandleren har givet de relevante garantier for så vidt angår implementeringen af tekniske og organisatoriske sikkerhedsforanstaltninger til beskyttelse af personoplysninger.

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 instruksen 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.
3. Er den dataansvarliges instruks efter databehandlerens rimelige vurdering ulovlig, kan databehandleren ophøre med videre behandling end opbevaring, indtil den dataansvarlige afgiver supplerende instruks. Databehandlerens ophør af behandlingen anses ikke for misligholdelse af disse Bestemmelser eller Hovedaftalen.

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.
3. Fortrolighedsforpligtelsen gælder ligeledes efter disse Bestemmelsers ophør.

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 og gennemføre foranstaltninger, herunder:

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.

2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene og gennemføre foranstaltninger for at imødegå disse. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren.
3. Databehandleren bistår den dataansvarlige med vedkommendes overholdelse af forpligtelsen efter forordningens artikel 32. Hvis imødegåelse af de identificerede risici 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 databeskyttelsesforordningens 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 generel skriftlig godkendelse fra den dataansvarlige.
3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel, og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Den dataansvarlige kan alene gøre indsigelse, hvis der foreligger rimelige og konkrete årsager hertil relateret til databeskyttelse. Listen over godkendte underdatabehandlere fremgår af bilag B.

Manglende underretning om nye underdatabehandlere kan udgøre et brud på persondatasikkerheden, idet personoplysninger i så fald videregives til en modtager, som den dataansvarlige ikke har autoriseret. Databehandleren er forpligtet til at sikre, at underretning sker rettidigt forud for ibrugtagning af enhver ny underdatabehandler.

4. Når databehandleren gør brug af en underdatabehandler, skal databehandleren pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser. Databehandleren er ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.
5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold, skal ikke sendes til den dataansvarlige.
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.

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 kræves i henhold til EU-ret eller national ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning.

3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren ikke:

   a) overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
   b) overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
   c) behandle personoplysningerne i et tredjeland

4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, 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 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.

Hvis en registreret fremsætter anmodning direkte til databehandleren, videresender databehandleren uden ugrundet ophold anmodningen til den dataansvarlige. Databehandleren besvarer ikke sådanne anmodninger, medmindre den dataansvarlige har autoriseret dette.

Bistand omfatter navnlig overholdelse 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. Databehandleren bistår endvidere den dataansvarlige med:

a) anmeldelse af brud på persondatasikkerheden til Datatilsynet senest 72 timer efter at den dataansvarlige er blevet bekendt hermed
b) underretning af registrerede om brud på persondatasikkerheden med høj risiko
c) gennemførelse af konsekvensanalyser
d) forudgående høring af Datatilsynet, såfremt en konsekvensanalyse viser høj risiko

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.

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. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 48 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin 72-timers anmeldepligt til Datatilsynet, jf. databeskyttelsesforordningens artikel 33.

3. Databehandleren bistår den dataansvarlige med at tilvejebringe følgende information til anmeldelsen:

a) karakteren af bruddet, herunder kategorierne og det omtrentlige antal berørte registrerede samt berørte registreringer af personoplysninger
b) de sandsynlige konsekvenser af bruddet på persondatasikkerheden
c) de foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet, herunder foranstaltninger for at begrænse dets mulige skadevirkninger.

4. Parterne angiver i bilag C den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til anmeldelse af brud.

11 Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne er databehandleren forpligtet til at slette alle personoplysninger fra aktive systemer senest 30 dage efter aftalens ophør og bekræfte over for den dataansvarlige, at oplysningerne er slettet – medmindre EU-retten eller national ret foreskriver opbevaring. Personoplysninger kan dog forekomme i tekniske sikkerhedskopier i op til 90 dage efter sletning fra aktive systemer som led i normale backup-cyklusser, hvorefter de overskrives eller slettes automatisk.
2. Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

12 Revision, herunder inspektion

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 angivet 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, 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 andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

14 Ikrafttræden og ophør

1. Disse Bestemmelser træder i kraft ved indgåelsen af Hovedaftalen og accepteres automatisk heri.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder giver anledning hertil. Firma360 ApS er berettiget til at opdatere denne Aftale med 30 dages varsel via offentliggørelse på https://firma360.dk/dba/.
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, aftales mellem parterne.
4. Hvis levering af tjenesterne ophører, og personoplysningerne er slettet i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.
5. Aftalen er underlagt dansk ret, og enhver tvist forelægges en dansk domstol.

15 Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner. Databehandlerens kontaktperson er: Jim Sandholm, dba@firma360.dk. Kontaktpersonen hos den dataansvarlige fremgår af Hovedaftalen.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

[1] Henvisninger til "medlemsstat" i disse bestemmelser skal forstås som en henvisning til "EØS-medlemsstater".

BILAG A – Oplysninger om behandlingen

A.1. Formålet med databehandlerens behandling af personoplysninger

Firma360 ApS behandler personoplysninger på den dataansvarliges vegne i forbindelse med levering af én eller flere af følgende ydelser:

- **Webhosting og drift:** Hosting af hjemmesider, webshops og applikationer, herunder backup, overvågning, vedligehold og support.
- **Webudvikling og appudvikling:** Design, udvikling, test og vedligehold af hjemmesider, webshops og applikationer til bl.a. Apple App Store og Google Play Store.
- **Marketing og annoncering:** Planlægning, udførelse og optimering af digitale marketingaktiviteter, herunder e-mailmarketing, annoncering på sociale medier og søgemaskiner samt sporing og analyse af kampagneresultater.
- **Konsulentydelser:** Specifikt aftalte opgaver inden for digital forretningsudvikling, herunder rådgivning, analyse og implementering af digitale løsninger.

A.2. Karakteren af behandlingen

Behandlingen kan omfatte organisering, systematisering, facilitering, midlertidig opbevaring, filtrering, tilpasning, genfinding, brug, sammenstilling, begrænsning og/eller sletning af personoplysninger i forbindelse med opfyldelse af de aftalte ydelser.

A.3. Typer af personoplysninger

Almindelige personoplysninger (artikel 6), herunder typisk:

- Kontaktoplysninger (navn, e-mailadresse, telefonnummer, adresse)
- Loginoplysninger og brugerdata
- Transaktions- og ordredata
- IP-adresser og cookie-/sporingsdata
- Adfærdsdata genereret via hjemmesider og apps
- CPR-nummer via EAN-fakturering (behandles som fortrolig oplysning)

Særlige kategorier (artikel 9): Behandles alene i det omfang, det er specificeret og skriftligt aftalt særskilt med den dataansvarlige.

A.4. Kategorier af registrerede

- Den dataansvarliges slutbrugere og kunder
- Den dataansvarliges kunders slutbrugere
- Den dataansvarliges medarbejdere
- Den dataansvarliges kontaktpersoner og samarbejdspartnere

A.5. Varighed

Behandlingen påbegyndes, når Hovedaftalen træder i kraft, og ophører, når Hovedaftalen ophører, jf. Bestemmelse 11 og Bilag C.4.

BILAG B – Underdatabehandlere

B.1. Godkendte underdatabehandlere

Den til enhver tid opdaterede liste er tilgængelig på: https://firma360.dk/dba/

Navn	Land	Funktion	Tredjeland	Grundlag
Simply.com	DK	Webhosting	Nej	–
Hetzner Online GmbH	DE	Webhosting / servere	Nej	–
Amazon Web Services (AWS)	US	Cloud hosting / infrastruktur	Ja	DPF/SCC
Vercel Inc.	US	Hosting / deployment (webapps)	Ja	SCC
Supabase	US	Databasehosting / backend	Ja	SCC
Google Firebase	US	Backend / databasehosting	Ja	DPF/SCC
Punktum dk (DK-Hostmaster)	DK	Domænehåndtering	Nej	–
WordPress (Automattic)	US	CMS-platform	Ja	DPF/SCC
WooCommerce (Automattic)	US	E-handelsplatform	Ja	DPF/SCC
Dropbox	US	Filopbevaring	Ja	DPF/SCC
Microsoft (365, Azure, Bing)	US	Filopbevaring, e-mail, annoncering	Ja	DPF/SCC
Google (Ads, Analytics, Workspace, Gemini)	US	Annoncering, sporing, e-mail, AI	Ja	DPF/SCC
Meta Platforms (Facebook & Instagram)	US	Annoncering, sporing	Ja	DPF/SCC
LinkedIn	US	Annoncering, sporing	Ja	DPF/SCC
WeTransfer	EU	Filoverførsel	Nej	–
Adobe Inc.	US	Kreativværktøjer / analytics	Ja	DPF/SCC
Active Campaign	US	E-mailmarketing, automatisering	Ja	SCC
Klaviyo	US	E-mailmarketing, SMS, annoncering	Ja	DPF/SCC
Drip	US	E-mailmarketing, automatisering	Ja	SCC
HubSpot	US	CRM, e-mailmarketing, annoncering	Ja	DPF/SCC
OneSignal	US	Push-notifikationer	Ja	SCC
Make (tidl. Integromat)	EU/CZ	Automatisering / integrationer	Nej	–
Zapier	US	Automatisering / integrationer	Ja	SCC
n8n	DE	Automatisering / integrationer	Nej	–
Effihub	DK	Automatisering / integrationer	Nej	–
Apple Inc. (APNs & TestFlight)	US	Push-notif. og betadistribution af apps	Ja	SCC
Google LLC (Firebase Cloud Messaging)	US	Push-notifikationer til Android-apps	Ja	DPF/SCC
Anthropic (Claude API)	US	AI-assisteret indholdsproduktion og analyse	Ja	SCC
OpenAI (ChatGPT API)	US	AI-assisteret indholdsproduktion og analyse	Ja	SCC
Dinero	DK	Regnskab og fakturering	Nej	–
Stripe	US	Betalingsgateway	Ja	DPF/SCC
Clearhaus	DK	Indløser	Nej	–
Quickpay	DK	Betalingsgateway	Nej	–
Flatpay	DK	Betalingsløsning	Nej	–

__DPF__ = EU-U.S. Data Privacy Framework · __SCC__ = EU-standardkontraktbestemmelser. AI-tjenester anvendes via API/Business-planer med indgået DPA. Apple App Store og Google Play Store agerer som selvstændige dataansvarlige og fremgår ikke af listen.

B.2. Varsel og procedure for ændringer

Underretning om tilføjelse eller udskiftning af underdatabehandler sker med minimum 30 dages varsel via direkte e-mail til den dataansvarliges kontaktperson og offentliggørelse på https://firma360.dk/dba/.

Den dataansvarlige kan gøre indsigelse inden ændringens virkningstidspunkt, såfremt der foreligger rimelige og konkrete årsager relateret til databeskyttelse. I særlige tilfælde med akut behov for udskiftning underretter databehandleren den dataansvarlige snarest muligt og senest ved ibrugtagning.

BILAG C – Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling sker ved udførelse af de ydelser, der er beskrevet i Bilag A og Hovedaftalen.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet afspejler karakteren af de behandlede personoplysninger og de aftalte ydelser. Databehandleren gennemfører som minimum følgende foranstaltninger:

C.2.1. Organisatorisk sikkerhed

- Dokumenteret informationssikkerhedspolitik der forankrer informationssikkerhed i organisationen.
- Medarbejdere med adgang til personoplysninger er underlagt fortrolighedsforpligtelser og modtager løbende undervisning i databeskyttelse.
- Tredjepartsleverandører er underlagt fortrolighedsforpligtelser og databeskyttelseskrav inden ibrugtagning.
- Databeskyttelse gennem design og standardindstillinger iagttages i alle faser af systemers og oplysningers livscyklus.
- Skrotning af dataudstyr foretages af samarbejdspartnere, der sikrer dokumenteret datasletning.

C.2.2. Fysisk sikkerhed

- Lokationer med adgang til personoplysninger er beskyttet med passende fysisk adgangskontrol.
- Bortskaffelse af fysiske datamedier sker sikkert i overensstemmelse med anerkendte branchestandarder.
- Fysisk adgang til systemer, der behandler personoplysninger, logges.

C.2.3. System- og netværkssikkerhed

- Antivirus installeret og løbende opdateret på alle systemer og databaser.
- Netværk og enheder beskyttet mod uautoriseret adgang via firewalls og indbrudssikringssystemer.
- Interne netværk segmenteret, så adgang til systemer og databaser med personoplysninger begrænses.
- Sikkerhedsopdateringer og patches udrulles rettidigt på alle relevante systemer.
- Løbende sårbarhedsscanninger og penetrationstests af relevante systemer.
- Kryptering ved transmission af fortrolige personoplysninger (minimum TLS 1.2).

C.2.4. Adgangsstyring

- Adgang til personoplysninger begrænset til brugere med arbejdsbetinget behov (least privilege).
- MFA (multifaktor-godkendelse) anvendes for fjernadgang til systemer med personoplysninger.
- Logning af aktivitet og sikkerhedshændelser. Logdata opbevares i minimum 12 måneder.

C.2.5. Sikkerhedskopiering og gendannelse

- Regelmæssig krypteret backup, opbevaret adskilt fra den primære databehandling.
- Personoplysninger kan forekomme i sikkerhedskopier i op til 90 dage efter sletning fra aktive systemer, hvorefter de overskrives eller slettes automatisk.

C.2.6. Beredskab og hændelseshåndtering

- Dokumenterede procedurer til opdagelse, analyse og håndtering af sikkerhedshændelser.
- Persondatasikkerhedsbrud registreres og rapporteres til den dataansvarlige jf. Bestemmelse 10.

C.2.7. Testmiljøer

- Personoplysninger i test er altid pseudonymiserede eller anonymiserede.
- Produktionsmiljøer er adskilt fra test- og udviklingsmiljøer.

C.3. Bistand til den dataansvarlige

- Databehandleren videresender uden ugrundet ophold anmodninger fra registrerede til den dataansvarlige.
- Databehandleren bistår efter specifik anmodning med de registreredes rettigheder, underretning om sikkerhedsbrud, konsekvensanalyser og forudgående høringer.
- Bistand ud over sædvanlig service afregnes særskilt, jf. Bilag D.5.

C.4. Opbevaringsperiode/sletterutine

Ved ophør sletter databehandleren alle personoplysninger fra aktive systemer senest 30 dage efter aftalens ophør og bekræfter dette skriftligt – medmindre gældende lovgivning foreskriver fortsat opbevaring. Personoplysninger kan forekomme i tekniske sikkerhedskopier i op til 90 dage, hvorefter de overskrives eller slettes automatisk.

C.5. Lokalitet for behandling

- Firma360 ApS, Vandtårnsvej 106B, 2860 Søborg (primær lokation)
- Lokationer hos godkendte underdatabehandlere, jf. Bilag B
- Den dataansvarliges lokationer, i det omfang det er nødvendigt for opgavens udførelse

C.6. Instruks vedrørende overførsel til tredjelande

C.6.1. Generel godkendelse – sikre tredjelande

Den dataansvarlige giver sin generelle godkendelse til overførsel til tredjelande med tilstrækkeligt beskyttelsesniveau (artikel 45) og til organisationer i USA certificeret under EU-U.S. Data Privacy Framework (DPF).

C.6.2. Godkendelse af specifikke modtagere

Den dataansvarlige instruerer databehandleren til at overføre personoplysninger via de underdatabehandlere, der er angivet i Bilag B.1. Databehandleren er bemyndiget til at anvende de til enhver tid gældende EU-standardkontraktbestemmelser (SCC).

C.7. Procedurer for den dataansvarliges revisioner

C.7.1. Tilsynskoncept og frekvens

Tilsyn kan gennemføres i én af følgende former, højst én gang om året, medmindre lovgivning kræver hyppigere tilsyn:

- **Tilsynskoncept 1 – Egenkontrol:** Skriftlig anmodning om dokumentation (IT-sikkerhedspolitik, risikovurderinger, beredskabsplaner) til dba@firma360.dk.
- **Tilsynskoncept 2 – Fysisk inspektion:** Kræver skriftlig aftale minimum 4 uger forud. Finder sted i normal kontortid.
- **Tilsynskoncept 3 – Spørgeskema:** Den dataansvarlige fremsender et spørgeskema, som besvares skriftligt inden en aftalt frist. Udgør i de fleste tilfælde den primære tilsynsform.

Eksisterende ISAE- eller ISO 27001-erklæringer inden for de seneste 12 måneder kan erstatte ny revision af allerede dækkede foranstaltninger.

C.7.2. Omkostninger ved tilsyn

Den dataansvarliges udgifter ved fysisk tilsyn afholdes af den dataansvarlige. Databehandleren stiller den nødvendige tid og de nødvendige ressourcer til rådighed.

C.8. Procedurer for revision af underdatabehandlere

Databehandleren fører løbende tilsyn med underdatabehandlere via en risikobaseret tilgang, herunder gennemgang af revisionserklæringer (ISAE, ISO 27001 eller tilsvarende), spørgeskemaer og om nødvendigt fysisk inspektion. Dokumentation fremsendes til den dataansvarlige efter anmodning.

BILAG D – Parternes regulering af andre forhold

D.1. Generelt

I tilfælde af uoverensstemmelse mellem Bestemmelserne og Bilag D har Bilag D forrang, medmindre bestemmelsen er ufravigelig i henhold til databeskyttelsesforordningen.

D.2. Konsekvenser af den dataansvarliges ulovlige instruks

Er instruksen efter databehandlerens rimelige vurdering ulovlig, kan databehandleren ophøre med videre behandling end opbevaring, indtil supplerende instruks afgives. Ophøret anses ikke for misligholdelse. Den dataansvarlige skadesløsholder databehandleren for krav som direkte følge af behandling udøvet efter instruksen.

D.3. Implementering af alternative sikkerhedsforanstaltninger

Databehandleren er berettiget til at implementere alternative sikkerhedsforanstaltninger, forudsat at disse giver mindst samme sikkerhedsniveau.

D.4. Anvendelse af underdatabehandlere, der leverer på standardvilkår

Hvis en underdatabehandler leverer på egne standardvilkår, som databehandleren ikke kan fravige, gælder disse vilkår for de pågældende behandlingsaktiviteter. Den dataansvarlige giver herved sin accept heraf, i det omfang standardvilkårene er forenelige med databeskyttelsesforordningen.

D.5. Vederlag for databehandlerens bistand og ydelser

Følgende bistand ydes uden særskilt vederlag som del af den lovpligtige bistandspligt:

- Grundlæggende bistand til besvarelse af anmodninger fra registrerede
- Underretning om persondatasikkerhedsbrud
- Besvarelse af spørgeskema (tilsynskoncept 3) én gang om året

Øvrig bistand afregnes efter medgået tid på baggrund af aftalte timesatser i Hovedaftalen med tillæg af direkte afholdte omkostninger, herunder:

- Udvidet bistand til anmodninger fra registrerede og tilsynsmyndigheder
- Fysisk inspektion (tilsynskoncept 2) og dokumentationsudarbejdelse hertil
- Gennemførelse af konsekvensanalyser efter specifik anmodning
- Ændringer af instruksen

D.6. Ansvar og ansvarsbegrænsning

Ansvarsbegrænsningen i Hovedaftalen finder anvendelse for databehandlerens behandling af personoplysninger under disse Bestemmelser samt med hensyn til artikel 82 i databeskyttelsesforordningen.

D.7. Krav fra de registrerede

Hver part hæfter for krav fra registrerede jf. artikel 82. Den dataansvarliges krav mod databehandleren kan ikke overstige ansvarsloftet i Hovedaftalen. Den dataansvarlige skadesløsholder databehandleren for krav, der overstiger ansvarsloftet i det omfang kravet skyldes den dataansvarliges egne handlinger eller undladelser.