Databehandleraftale

Standardkontraktsbestemmelser

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

mellem

Kunden (juridisk enhed) - som bruger af TimeView-platformen

herefter "den Dataansvarlige"

og

TimeSolutions A/S
CVR 30709810
Park Allé 295, 1.
2605 Brøndby
Danmark

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

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. I forbindelse med leveringen af ydelsen beskrevet i Bilag A 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 medlemsstaternes[1] 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. 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.

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

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 afden 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 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 45 dages varsel og derved give den Dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af

de(n) omhandlede underdatabehandler®. Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den Dataansvarlige allerede har godkendt, fremgår af bilag B.

4. Når Databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den Dataansvarlige, skal Databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.
   Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder Databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.
5. Underdatabehandleraftale® 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.
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 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, 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 muligt skal bistå den Dataansvarlige i forbindelse med, at den Dataansvarlige skal sikre overholdelsen af:

a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
c. indsigtsretten
d. retten til berigtigelse
e. retten til sletning ("retten til at blive glemt")
f. retten til begrænsning af behandling
g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
h. retten til dataportabilitet
i. retten til indsigelse
j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

2. I tillæg til Databehandlerens forpligtelse til at bistå den Dataansvarlige i henhold til Bestemmelse 6.3., bistår Databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Databehandleren, den Dataansvarlige med:
    a. den Dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til Datatilsynet, medmindre 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 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. Databehandlerens underretning til den Dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den Dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.
3. I overensstemmelse med Bestemmelse 9.2.a skal Databehandleren bistå den Dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at Databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den Dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:
    a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
    b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
    c. de foranstaltninger, som den Dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.
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 at tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

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, 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 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. Bestemmelserne træder i kraft samme tidspunkt som Licensbetingelser for brug af TimeView.
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.

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.

<u>På vegne af den Dataansvarlige:</u>	<u>På vegne af Databehandleren:</u>	
Den Dataansvarlige er ansvarlig for at opdatere kontaktpersonen hos Databehandleren. Ændring af kontaktperson skal ske til: dpo@timesolutions.dk.	Navn	Thorkild Eriksen
	Stilling	Adm. direktør
	Telefonnummer	7070 1011
	E-mail	dpo@timesolutions.dk

Bilag A Oplysninger om behandlingen

A.1. Formålet med Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige

Databehandleren behandler personoplysninger udelukkende med det formål at levere og vedligeholde det aftalte system TimeView og dertilhørende funktionalitet til den Dataansvarlige, i overensstemmelse med den indgåede licensaftale

Systemet håndterer den Dataansvarliges kunder, kontakter og opgaver samt den tid, der anvendes af den Dataansvarlige på at løse disse opgaver. Den Dataansvarlige opretter selv data i systemet. Den Dataansvarliges medarbejdere registrerer deres arbejdstid på opgaver i systemet, det være sig tid forbrugt på kunder, afholdt ferie, afspadsering, sygdom og lignende.

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

Behandlingen omfatter de aktiviteter, der er nødvendige for driften, vedligeholdelsen og leveringen af TimeView, herunder men ikke begrænset til:

- Indsamling og registrering (via den Dataansvarlige)
- Opbevaring (hosting af data)
- Organisering og strukturering
- Søgning, udtrækning og sammenstilling
- Ændring og opdatering
- Sletning og tilintetgørelse
- Backup og gendannelse
- Teknisk support og fejlretning (som kan involvere adgang til data)
- Automatiserede e-mailudsendelser til ansatte og kunder for den Dataansvarlige

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

Behandlingen omfatter følgende typer af personoplysninger, som den Dataansvarlige uploader eller indtaster i TimeView:

- **Almindelige personoplysninger:**
    - Identifikationsoplysninger (f.eks. firmanavn, adresse, e-mail, telefonnummer)
    - Kontaktpersonoplysninger (f.eks. navn, e-mail, titel, telefon herunder også CPR-nummer for personlige selskaber)
    - Kommunikationshistorik (f.eks. noter fra møder, e-mailkorrespondance og lignende)
    - Købshistorik/salgsaktivitet
    - Tidsforbrug på opgaver
    - Interesser og præferencer (som indtastet af den Dataansvarlige)
    - Tidsforbrug for ansatte hos den Dataansvarlige herunder også sygdom, ferie, afspadsering etc.
- **Følsomme personoplysninger:**
    - TimeView er ikke egnet eller designet til at opbevare personoplysninger som beskrevet i GDPR artikel 9 & 10

A.4. Behandlingen omfatter følgende kategorier af registrerede

Behandlingen omfatter personoplysninger om følgende kategorier af registrerede:

- Kunder og potentielle kunder (f.eks. nuværende, tidligere, potentielle kunder)
- Leverandører og samarbejdspartnere
- Kontaktpersoner hos kunder, leverandører og samarbejdspartnere
- Ansatte hos den Dataansvarlige

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

Behandlingen af personoplysninger sker i hele Aftalens løbetid. Ved Aftalens ophør skal data slettes eller returneres i overensstemmelse med Aftalens vilkår og den Dataansvarliges instruks. Databehandleren opbevarer dog nødvendige logs og driftsdata i henhold til interne politikker og lovgivning, disse indeholder ikke personoplysninger, eller er anonymiseret.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den Dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	KONTAKTOPLYSNINGER	FORMÅL / YDELSE	DATA	3. LANDS-OVER.
Hosting, Backup & Infrastruktur				
Microsoft Azure	Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland	Hosting og backup	NL	Ja, Data Privacy Framework
Postmark	AC PM LLC, 1 N Dearborn Street, Suite 500, Chicago, IL 60602, USA	E-mail levering	USA	Ja, Data Privacy Framework
4Ing	4Ing ApS, Rundingen 16, Herringløse, 4000 Roskilde	Drift	DK	
Support & Service				
Intercom	Intercom, Inc., 55 2. street suite 400, CA94105 San Francisco, USA	Supportsystem	USA	Ja, Data Privacy Framework
TeamViewer GmbH	TeamViewer GmbH, Göppingen, Bahnhofsplatz 2, Germany	Supportassistance	EU	
Microsoft Office 365	Microsoft Corporation 1 Microsoft Way Redmond, WA 98052 USA	E-mail	EU	Ja, Data Privacy Framework
4Ing	4Ing ApS, Rundingen 16, Herringløse, 4000 Roskilde	Support	DK	
TimeSolutions kundehåndtering				
Visma e-conomic A/S	Gærtorvet 1, 5 1799 København V	ERP & fakturering	IE	Ja, Data Privacy Framework
TimeManagement ApS	Kirkebjerg Parkvej 12 2605 Brøndby	Bogholderiservice	DK	
Lexoforms A/S	Vejlsøvej 51, bygning O 8600 Silkeborg	DPA håndtering	DK	
TimeView	TimeSolutions A/S Park Allé 295, 1. 2605 Brøndby	Kundehåndtering	NL	

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

B.2. Varsel for godkendelse af underdatabehandlere

Databehandleren har tilladelse til at anvende underdatabehandlerne beskrevet i B.1.

Ændringer til underdatabehandlere skal notificeres til Dataansvarlige på følgende måde:

Generelt notificeres med 30 dage fra underdatabehandlerne til Databehandleren. Databehandleren notificerer hurtigst muligt den Dataansvarlige mhp. eventuelle indsigelse(r) mod underdatabehandlere.

For Intercom notificeres med 20 dages varsel, som Databehandleren videresender notifikation til den Dataansvarlige hurtigst muligt efter.

For TeamViewer notificeres med 15 dages varsel, som Databehandleren videresender notifikation til den Dataansvarlige hurtigst muligt efter.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige sker som opfyldelse af Licensaftale mellem den Dataansvarlige og Databehandler.
Databehandleren har implementeret følgende tekniske og organisatoriske foranstaltninger for at sikre fortrolighed, integritet, robusthed og tilgængelighed af de personoplysninger, der behandles via TimeView, og som beskrevet i A.3.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle data som beskrevet i A.3.

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.

Adgangskontrol

- Adgang til systemet lægger op til brugernavn og stærk adgangskode (sættes af Dataansvarlige).
- Mulighed for aktivering af to-faktor-autentifikation (2FA) for brugere.
- Adgang for medarbejdere hos Databehandleren er begrænset efter need-to-know-princippet.

Systemadskillelse

- Kundedata opbevares logiks adskilt i egne databaser.
- En kundes data kan ikke tilgås af andre kunder.
- Udvikling af systemet foregår på anonyme testdata.
- Driftsmiljøet er adskilt fra udviklings- og testmiljøer.

Kryptering

- Al datatrafik (f.eks. ved login og brug af systemet) krypteres via TLS (Transport Layer Security).
- Data i hvile opbevares krypteret (f.eks. AES-256).

Backup og datagendannelse

- Regelmæssig automatisk backup af data.
- Backups opbevares sikkert og testet for gendannelsesprocedurer (Restore testes halvårligt).
- Mulighed for at reetablere personoplysninger i tilfælde af tekniske hændelser.

Databehandlerens medarbejdere

- Medarbejdere har tavshedspligt og er instrueret i håndtering af personoplysninger.
- Der gennemføres løbende orientering i datasikkerhed og GDPR.

Fysisk sikkerhed

- Hosting sker i sikre datacentre med fysisk adgangskontrol.
- Databehandleren arbejder papirløst

Logning og overvågning

- Systemet logger adgang og ændringer i data til sikkerhedsmæssig kontrol og fejlsøgning.
- Logfiler kontrolleres ved mistanke om uautoriseret adgang.

Sårbarhedsstyring og opdatering

- Regelmæssig opdatering af software og underliggende systemer.

- Der afvikles periodevist penetrationtest af computere og systemer.
- Overvågning for sikkerhedshuller og hurtig håndtering af kritiske sårbarheder.

Håndtering af brud på persondatasikkerheden
- Interne procedurer for identifikation, håndtering og rapportering af sikkerhedsbrud.
- Meddelelse til den Dataansvarlige uden unødig forsinkelse ved konstateret brud (9.2 og C.3).

Best practice
- Databehandleren følger forskrifter for opsætning og drift fra leverandører
- Anbefalinger fra leverandører gennemgås og anvendes hvor muligt
- Firewalls er opsat og konfigureret efter forskrifter

API
- API adgang styres for den Dataansvarlige via en af to muligheder:
    - API key
    - Microsoft entraID
- Adgangen styres via den tildelte rolle for nøglen
- Al adgang via API logges

C.3 Bistand til den Dataansvarlige
Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den Dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre de i C.2 tekniske og organisatoriske foranstaltninger.

C.4 Opbevaringsperiode/sletterutine
Data og personoplysninger opbevares i systemet indtil disse slettes af den Dataansvarlige. Databehandleren kan under instruks assistere den Dataansvarlige hermed.

Ved ophør af licensaftalen 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:

- EU
- USA

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Databehandleren overfører ikke personoplysninger til tredjelande, undtagen til de generelt godkendte underdatabehandlere listet i Bilag B.

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

Databehandleren sikrer kontrol af overholdelse af sine forpligtelser i henhold til denne Databehandleraftale og artikel 28 i GDPR gennem følgende foranstaltninger:

Intern Kontrol:
Intern Audit: Databehandleren udfører regelmæssige interne audits af sine informationssikkerhedsprocesser og -kontroller for at sikre overholdelse af interne politikker og gældende lovgivning, herunder GDPR. Resultaterne heraf er genstand for ledelsens gennemgang.

Den Dataansvarliges Auditret:
Adgang til Dokumentation: Databehandleren vil efter anmodning og med rimeligt varsel stille den nødvendige information og dokumentation til rådighed for den Dataansvarlige til demonstration af overholdelse af denne aftale og artikel 28 i GDPR.

Audit udført af den Dataansvarlige:
I det omfang den Dataansvarliges rettigheder til audit ikke fuldt ud kan opfyldes gennem adgang til tredjepartsrapporter og anden dokumentation, og der foreligger en specifik, saglig og dokumenteret mistanke om manglende overholdelse, kan den Dataansvarlige anmode om at udføre en audit.

Auditbetingelser:
En sådan audit skal varsles med 30 dage skriftligt. Auditens omfang, varighed og tidspunkt skal aftales i gensidig forståelse og må ikke unødigt forstyrre Databehandlerens drift eller kompromittere sikkerheden for andre kunders data. Omkostningerne ved en sådan audit afholdes af den Dataansvarlige.

Begrænset adgang:
Auditretten omfatter ikke direkte adgang til Databehandlerens produktionsmiljø, andre kunders data, kildekode eller informationer, der kompromitterer Databehandlerens intellektuelle ejendomsret eller forretningshemmeligheder, medmindre andet er specifikt aftalt og nødvendigt for auditens formål. Adgang til data er begrænset til den Dataansvarliges egne data, og kun i det omfang det er teknisk muligt og nødvendigt for auditens formål.

Audit-resultater:
Resultater af auditten deles med Databehandleren, som forpligter sig til at udbedre eventuelle fundne mangler inden for en rimelig tidsramme.

Audit udført af uafhængig tredjepart på den Dataansvarliges vegne:
Den Dataansvarlige kan vælge at lade en uafhængig tredjepart udføre auditten på den Dataansvarliges vegne, forudsat at denne tredjepart er anerkendt, kvalificeret og underskriver en fortrolighedsaftale med Databehandleren. Betingelserne i punkt ” Audit udført af den Dataansvarlige” gælder tilsvarende for en sådan tredjeparts-audit.

Databehandleren forpligter sig til at samarbejde med den Dataansvarlige og Datatilsynet i det omfang, det er nødvendigt for at opfylde den Dataansvarliges forpligtelser i henhold til GDPR, herunder ved tilsyn eller anmodninger fra tilsynsmyndigheder.

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

Databehandlerens revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til underdatabehandleren, sker på samme måde som den Dataansvarliges revisioner hos Databehandleren, se punkt C.7.