DATABEHANDLERFTALE

mellem

KUNDENS [NAVN]
CVR [CVR-NR]
[ADRESSE]
[POSTNUMMER OG BY]

herefter "den dataansvarlige"

og

Vitec MV A/S
CVR-nr. 15 31 44 00
Edisonsvej 4
5000 Odense C

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 ... 3
3. Den dataansvarliges rettigheder og forpligtelser ... 3
4. Databehandleren handler efter instruks ... 4
5. Fortrolighed ... 4
6. Behandlingssikkerhed ... 4
7. Anvendelse af underdatabehandlere ... 5
8. Overførsel til tredjelande eller internationale organisationer ... 6
9. Bistand til den dataansvarlige ... 7
10. Underretning om brud på persondatasikkerheden ... 8
11. Sletning og returnering af oplysninger ... 8
12. Revision, herunder inspektion ... 8
13. Parternes aftale om andre forhold ... 9
14. Ikrafttræden og ophør ... 9
15. Kontaktpersoner hos den dataansvarlige og databehandleren ... 10
Bilag A Oplysninger om behandlingen ... 11
Bilag B Underdatabehandlere ... 15
Bilag C Instruks vedrørende behandling af personoplysninger ... 15
Bilag D Parternes regulering af andre forhold ... 18

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 ydelse i henhold til Hovedkontrakten af [dato] samt eventuelle senere tillæg 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.

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

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.

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 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). 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(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.

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 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. 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 slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlige, at oplysningerne er slettet medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

2. Revision, herunder inspektion (Pkt 12)

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.

12. 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.

13. 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	Hans-Erik Schou
Stilling	CEO
Telefonnummer	65 91 80 22
E-mail	hans-erik.schou@vitecsoftware.com
Underskrift	

14. 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	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-mail	[E-MAIL]

Bilag A Oplysninger om behandlingen

Databehandler yder som led i opfyldelse af Hovedkontrakten levering af følgende digitale hjælpemidler/software- produkter til den dataansvarlige:

- CD-ORD
- IntoWords

Databehandlers softwareprodukter støtter og forenkler "behandling af tekst" for en given bruger. Behandling af tekst skal forstås som disse processer:

- Tekstforståelse: Produktet hjælper bruger med at forstå skrevet tekst ved hjælp af teknikker som oplæsning og opmærkning af tekst for brugeren
- Udarbejdelse af tekst: Bruger støttes med ordforslag og stavehjælp
- Indtaling – Tale til Tekst: Tekst genereres på baggrund af indtaling. Konvertering af tale til tekst sker ved API kald til en tredjeparts service.

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

Produkternes services:
Formålet med at behandle personoplysninger i forbindelse med brugen af databehandlers produkter er at yde den aftalte service samt at optimere produkternes performance, herunder skabe den bedste læring-, læse- og skrivestøtte for bruger af produkterne/services, der herved opnår støtte til at "læse og forstå en tekst", "skrive en tekst" samt "tale en tekst".

For at produkterne kan yde brugeren støtte i nævnte, skal der for hver bruger oprettes en konto-/brugeradgang. Denne log in/registrering af bruger medvirker til, at produktet udarbejder en statistik for den pågældende bruger. Dette sker ved, at produkterne/services ved brug registrerer brugerens handlinger, herunder hvor mange ordforslag, brugeren foreslås, at der sker tekstoplæsning samt at billeder konverteres til tekst. Hvilke ord og billeder, der er tale om, registreres dog ikke. Det er således funktionen, der registreres, men ikke indholdet af funktionerne, der registreres.

Slutbrugerstatistik:
Ved brug af services sker der yderligere behandling af brugers persondata med det formål at skabe en slutbrugerstatistik. Statistik tilknyttet slutbrugeren er alene baseret på antallet af anvendelser af services (herunder antal ordforslag givet samt antal oplæsninger af tekst). Produkterne registrerer ikke indhold eller karakter af tekst foreslået/oplæst. Slutbruger har mulighed for at se sin egen statistik.

Statistik til brug for forbedring af produkterne:
Til databehandlers interne evaluering af produkterne, indsamles statistik kumuleret for alle brugere af databehandlers systemer. Denne statistik er anonymiseret og afkobles helt fra slutbrugeren. Databehandler kan fra statistikken udlede, hvor mange ordforslag, der gives på en given dag eller tidspunkt på døgnet, men ikke i relation til den specifikke bruger.

Særligt om Indtaling – Tale til Tekst
Konvertering af tale til tekst sker ved brug af Microsoft Azure, der udbydes af Microsoft. Når databehandler modtager lydfilen med brugerens indtaling, sender databehandler lydfilen,

sammen med andre brugeres lydfiler, til Microsoft i Holland via et API med henblik på konvertering til tekst. Lydfilen slettes øjeblikkeligt efter, at Microsoft har konverteret den.

Der sendes ikke andre oplysninger sammen med lydfilen, og Microsoft har således ingen mulighed for at koble lydfilen sammen med den bruger, der har indtalt lydfilen, og dermed heller ingen mulighed for at identificere den pågældende bruger. Mens lydfilen er i Microsofts besiddelse, er der således ikke tale om en oplysning, der er personhenførbar, og der er dermed heller ikke tale om behandling af en personoplysning. Microsoft behandler således ikke på noget tidspunkt brugerens personoplysninger og er dermed ikke underdatabehandler for databehandler.

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

Databehandlerens behandling af personoplysninger drejer sig primært om, på vegne af den dataansvarlige, at autentificere login oplysninger, herunder Unilogin oplysninger m.fl.

Databehandlers produkter indsamler og registrerer data om brugeren ved oprettelse af log in-/brugerkonto samt ved brugen af produktet/services for at levere den aftalte ydelse.

Ved Erhverv- og Privatkunde registreres navn og e-mail på bruger for at oprette brugeradgang. Data opbevares så længe brugeradgang er aktiv. Herefter anonymiseres og slettes data.

Ved Kommune-kunde er data pseudonymsieret. Navn og e-mail på bruger registreres midlertidigt under login-processen. Disse data opbevares så længe brugeradgang er aktiv, dvs. den aktive brugersession, eksempelvis 30min. Brugerens login-hash fra idP gemmes permanent, dog kun så længe brugeren er tilknyttet databehandlers login, eller den underliggende kontrakt er aktiv. Statistisk data er pseudonymiseret og alene tilknyttet login-hash fra idP. Disse data slettes automatisk ved aftaleophør.

Ved brugen af databehandlers services registreres brugerens antal anvendelser af produkternes service for slutbrugerstatistikken. Der sker således registrering af antal ordforslag givet samt antal oplæsninger af tekst mv. Der sker ikke registrering af indhold eller karakter af tekst, der foreslås eller oplæses for brugeren.

Yderligere vedrørende log-in
For at anvende databehandlers services kræves oprettelse et gyldigt login. Login kan ske enten med et såkaldt federated login via en identity provider (idP) eller direkte via databehandlers brugerstyring. I sidstnævnte tilfælde fungerer databehandler som både login og idP.

Som oftest anvender Kommune- og Erhvervskunder federated login og private brugere anvender databehandler's brugerstyring. Fælles for federated logins er, at databehandler aldrig trækker mere data ved login, end der er nødvendigt for at levere LST til kunderne. Som oftest gemmes kun brugerens interne hash værdi. Det betyder, at brugere i databehandlers programmer er pseudonymiserede ved almindelig brug og databehandler kun kender til brugerens login. Det er ikke muligt for databehandler at henføre data til en specifik person, uden betydelig indsats. Såfremt eksempelvis en elev ved en given skole, bruger af databehandlers services, flytter kommune, vil det for databehandler være umuligt at afgøre, hvilken person det pseudonymiserede login har tilhørt uden samkøring med data fra UNI-C.

Fælles for alle data, der ikke er login/hash er, at de kun opbevares kortvarigt hos databehandler i forbindelse med login.

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

Fælles for alle type kunder er, at databehandler kun behandler almindelige personoplysninger, jf. GDPR Art 6, og således ikke personfølsomme personoplysninger, jf. GDPR Art 9.

Kommunekunder
Alle kommunekunder i Danmark anvender UNI-C, i Norge anvendes Feide, i Sverige anvendes Skolfederation og i Holland anvendes Entree. Ved login via disse idP'er stilles visse persondata til rådighed for databehandler. Dog anvendes disse data ikke og dataen gemmes ikke i databehandlers systemer. For enkelte offentlige kunder anvendes Google idP eller Microsoft idP, og i disse tilfælde udstilles kun tenant ID eller root domain. Disse oplysninger er at sidestille med Skolekode.

Data om bruger, der er er behov for/ stilles rådighed for databehandler ved login og service-brugen udgør følgende:

Data	Gemmes / anvendes ved login
Rolle	Ja
Navn	Nej
Adresse	Nej
Telefonnummer	Nej
E-mailadresse	Nej
Virksomhedsidentifikation	Nej
Kommunekode	Nej
Skolekode (Institutionsnummer)	Ja
Klassebetegnelse	Ja
Login / Hash	Ja

Erhvervskunder
I dette tilfælde fungerer login på samme måde som f.eks. ved UNI-C, men det er helt op til kunden, hvilke data, der medfølger ved log-in.

Data om bruger, der er behov for/ stilles til rådighed for databehandler ved login udgør følgende:

Data	Gemmes / anvendes ved login
Rolle	Ja
Navn	Nej
Adresse	Nej
Telefonnummer	Nej
E-mailadresse	Ja
Virksomhedsidentifikation	Ja
Kommunekode	Nej
Skolekode (Institutionsnummer)	Nej
Klassebetegnelse	Nej
Login / Hash	Ja

Private kunder
Ved kundens brug og anvendelse af databehandlers services er det nødvendigt at gemme personlige oplysninger direkte i databehandlers eget loginsystem.

Data om bruger, der er behov for/ stilles til rådighed for databehandler ved login udgør følgende:

Data	Gemmes / anvendes ved login
Rolle	Nej
Navn	Ja
Adresse	Ja
Telefonnummer	Ja
E-mailadresse	Ja
Virksomhedsidentifikation	Nej
Kommunekode	Nej
Skolekode (Institutionsnummer)	Nej
Klassebetegnelse	Nej
Login / Hash	Ja

A.4. Behandlingen omfatter følgende kategorier af registrerede

Ansatte tilknyttet dataansvarlige	
Elever tilknyttet dataansvarlige	
Kunder	
Børn i alderen 6-17 år.	
Kunder/private brugere	

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

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige påbegynder ved ikrafttrædelse af Hovedkontrakten og varer til senest 30 dage efter ophør af Hovedkontrakten, hvor databehandler har slettet alle dataansvarliges personoplysninger inden da.

Data for Private kunder slettes automatisk, når bruger-kontoen nedlægges af brugeren/kunden selv. Alle andre data vedrørende et bruger-login er efemerisk og opbevares kun hos databehandler, så længe brugeren er logget ind.

For sletning af specifikke slutbrugere hos Kommune- og Erhvervskunder, vil sletning afhænge af underretning fra dataansvarlige til databehandler, hvorefter der vil ske sletning.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere:

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Amazon Web Services		Dublin, Irland Greenhills Road, Tymon North, Dublin, Ireland	Serverhosting
Vitec Software Group, Koncern IT		Göteborg, Sverige	Serverhosting

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.

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:

Databehandler foranlediger, at dataansvarlige/dataansvarliges brugere kan oprette brugeradgang/login med henblik på, at denne bruger kan benytte de services som databehandlers produkter/services yder, jf. beskrivelse i Bilag A, herunder at databehandler registrerer dataansvarliges/brugers brug af service/produktet for slutbruger-statistik.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Behandlingen af personoplysninger forholder sig udelukkende til personoplysninger af almen karakter, jf. GDPR Art 6. Således behandles ingen personfølsomme oplysninger, jf. GDPR Art 9. Behandlingen omfatter dog en stor mængde personoplysninger af brugere, herunder af børn under 16 år.

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:

- Adgang til alle databehandlers systemer er sikret med MFA og alle databehandlers medarbejdere med adgang til driftsmiljøer har underskrevet en udvidet fortrolighedserklæring.
- Som primære driftsmiljø anvendes AWS i Irland, hvor data hostets, og hvor AWS indbyggede CloudTrail er aktiveret. Det betyder, at alle databehandlers medarbejderes log-ins og handlinger udført i driftsmiljøer bliver logget i 90 dage. Audit-log bliver løbende overvåget.
- Produkterne anvender både kryptering ”in transit” og ”at rest”. Det betyder blandt andet, at alle forbindelser til ”backend” er krypteret med TLS v1.3 ”in transit”. Kryptering ”at rest” afhænger af medie, men AES256 er oftest benyttet.
- Udstedelse af krypteringsnøgler og certifikater sker via Let’s Encrypt, AWS KMS eller ACM.
- Databehandler foretager løbende driftsovervågning af IT-systemer
- Adgang til databehandlers netværk sikres blandt andet ved brug af firewall, VPN-klient og beskyttet WiFi.

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 følgende tekniske og organisatoriske foranstaltninger:

På anmodning fra dataansvarlige kan databehandler slette og fremfinde alle statistiske data tilknyttet slutbrugeren. For Erhverv- og Kommunekunder forudsætter denne bistand, at oplysninger fra idP leveres af dataansvarlige, da databehandler ikke har direkte personhenførbare data for disses brugere.

For at slette data på vegne af den dataansvarlige kræves en række tekniske tiltag afhængig af brugertype:

Kommunekunder

Som udgangspunkt kan en specifik bruger ikke identificeres i databehandlers system, da der ikke opbevares direkte personhenførbare oplysninger på et brugerlogin. Det er derfor nødvendigt, at eksempelvis UNI-C kan udleveres af dataansvarlige for den specifikke brugers login / hash, således databehandler kan fremsøge denne i statistik-databasen.

Erhvervskunder
Brugeren kan identificeres ved hjælp af f.eks. e-mailadresse og kan slettes/fremfindes på baggrund af disse oplysninger.

Private kunder,
Brugeren kan identificeres ved hjælp af. f.eks. e-mailadresse, og data kan slettes/fremfindes på baggrund af disse oplysninger.

C.4 Opbevaringsperiode/sletterutine

Personoplysninger opbevares indtil en brugerkonto nedlukkes eller i perioden indtil Hovedkontrakten ophører og senest 30 dage herefter.
Privatkunder kan selv slette egen brugerkonto.

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:

Behandlingen af de af Bestemmelserne omfattede personoplysninger opbevares på følgende lokaliteter af følgende underdatabehandlere, der hoster data på vegne af databehandler:

- AWS-datacenter
  Greenhills Road, Tymon North, Dublin, Ireland

- Vitec software Group, Göteborg, Sverige

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.

Databehandleren forpligter sig til udelukkende at anvende underdatabehandlere, der befinder sig i EU eller sikre tredjelande.

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

Databehandleren skal hvert år for egen regning indhente en revisionserklæring fra en uafhængig tredjepart vedrørende databehandlerens 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 kan anvendes i overensstemmelse med disse Bestemmelser:

ISAE 3000 eller lignende.

Revisionserklæringen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering efter anmodning herom. Erklæringen offentliggøres desuden på databehandlers hjemmeside, www.vitec-mv.com

Baseret på resultaterne af erklæringen, 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.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt.

Anmodning om fysisk inspektion skal ske med mindst 30 dages varsel. Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren er forpligtet til at afsætte den tid, der er nødvendig for, at den dataansvarlige kan gennemføre sin inspektion. Dataansvarlige faktureres for databehandlerens anvendte tid og omkostninger for bundet med et sådan tilsyn, jf. timesatser angivet i bilag D.

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

Databehandleren skal jævnligt for egen regning hos underdatabehandlere indhente erklæringsrapporter eller lignende vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Bilag D Parternes regulering af andre forhold

Vederlag og omkostninger

Databehandleren har krav på betaling, efter medgået tid, for ydelser, der udføres af databehandler indenfor rammen af Bestemmelserne og dataansvarliges anmodning. Ydelserne kan omfatte, men er ikke begrænset til, ændringer af instruksen, assistance ved anmeldelse af brud på persondatasikkerheden, udlevering og sletning af oplysninger, bistand ved audit, bistand ved ophør, samarbejde med tilsynsmyndigheder og hjælp til efterlevelse af anmodninger fra registrerede.
Ydelserne kan også omfatte bistand til ændringer, der følger af nye risikovurderinger.

Databehandlers bistand afregnes således:

Konsulenttimepris: DKK 1.000 ex. moms

Priser reguleres i forhold til udviklingen i nettoprisindekset.

Ansvar og ansvarsbegrænsninger

Parternes ansvar for alle kumulerede krav i henhold til Bestemmelserne er begrænset til de samlede betalinger i henhold til Hovedkontrakten for den 12 måneders periode, der går umiddelbart forud for den skadegørende handling. Hvis Bestemmelserne ikke har været i kraft i 12 måneder, opgøres beløbet som den aftalte betaling af ydelser i henhold til Hovedkontrakten i den periode Bestemmelserne har været i kraft divideret med antallet af måneder, Bestemmelserne har været i kraft og derefter multipliceret med 12.

Force Majeure

Databehandleren kan ikke gøres ansvarlig for forhold, der almindeligvis må betegnes som force majeure, herunder, men ikke begrænset til, krig, optøjer, terror, opstand, strejke, ildsvåde, naturkatastrofer, valutarestriktioner, import- eller eksportrestriktioner, afbrydelse af almindelig samfærdsel, afbrydelse af eller svigt i energiforsyningen, offentlige dataanlæg og kommunikationssystemer, virus samt indtrædelse af force majeure hos underleverandører. Force majeure kan højst gøres gældende med det antal arbejdsdage, som force majeure-situationen varer.

Fortrolighed

Information vedrørende indholdet af disse Bestemmelser, den underliggende Hovedkontrakt, den anden Parts forretning, der enten i forbindelse med overgivelsen til den modtagende Part er angivet som fortrolig information, eller som efter sin natur eller i øvrigt klart må opfattes som fortrolig, skal behandles fortroligt og med mindst samme omhu og diskretion som partens egne fortrolige informationer. Data, herunder persondata, udgør altid fortrolige informationer.

Fortrolighedsforpligtelsen gælder dog ikke for information, som er eller bliver offentlig tilgængelig, uden dette skyldes brud på en Parts fortrolighedsforpligtelse eller information, som allerede er i den modtagende Parts besiddelse uden tilsvarende fortrolighedsforpligtelse eller information, som selvstændigt er udviklet af den modtagende Part.

Tvistløsning

Reguleringen af tvistløsning, som det fremgår af Hovedkontrakten, finder også anvendelse for disse Bestemmelser, som om Bestemmelserne var en integreret del af Hovedkontrakten.