Standardkontraktsbestemmelser (Databehandleraftale)

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

mellem

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

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.

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 af oplysninger 8
12. Revision, herunder inspektion 9
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 14
Bilag C Instruks vedrørende behandling af personoplysninger 16
Bilag D Parternes regulering af andre forhold 24

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 bestemmelser 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. Databehandleren skal, hvor muligt, i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette personoplysningerne.

7. 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 og Bilag B, B.1.

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 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.

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 lovgivning 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 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 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	Tove Larsen
Stilling	Konsulent
Telefonnummer	65 91 80 22
E-mail	Tove.Larsen@vitecsoftware.com
Underskrift	

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

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

Navn	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-mail	[E-MAIL]

Navn	Hans-Erik Schou
Stilling	Administrerende direktør
Telefonnummer	63 12 60 15
E-mail	support.mv@vitecsoftware.com

Bilag A Oplysninger om behandlingen

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

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:

CD-ORD:

- 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, stavehjælp.

IntoWords:

- 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, stavehjælp og Tale-til-tekst.
- Tale-til-tekst: Tekst genereres på baggrund af indtaling. Konvertering af tale til tekst sker ved API-kald til en tredjeparts service. Konvertering af Tale-til-tekst sker ved, at slutbruger transmitterer indtaling til databehandlers service, hvorefter databehandlers service transmitterer til MS Azure til behandling, hvorefter MS Azure transmitterer svar retur til databehandlerens service. Herefter transmitterer databehandlerens service retur til slutbrugeren med tekst. Lydfiler slettes automatisk både hos databehandleren og MS Azure efter, at den beskrevne behandling er afsluttet.
- Oversættelse: Oversættelse genereres ved, at slutbruger transmitterer tekst til databehandlers service, hvorefter databehandlers service transmitterer til Amazon til Behandling. Amazon transmitterer svar retur til databehandlers service. Herefter transmitterer databehandlers service retur til slutbruger med oversættelse. Tekst slettes automatisk både hos databehandleren og Amazon efter, at den beskrevne behandling er afsluttet.

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. med henblik på at levere de ydelser, som følger af A.1.

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

Ved Kommune-kunde er data pseudonymiseret. Brugerens login-hash fra idP gemmes permanent, dog kun så længe den underliggende kontrakt er aktiv.

Ved Erhvervskunder opretter kundens administrator selv brugerlogins.

Yderligere vedrørende log-in
For at anvende databehandlers services kræves oprettelse af 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. Fælles for federated logins er, at databehandler aldrig trækker mere data ved login, end der er nødvendigt for at levere produktet til kunderne. Der 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.

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

Kommunekunder
Alle kommunekunder i Danmark anvender UNI-C, i Norge anvendes Feide, i Sverige anvendes Skolfederation og i Holland anvendes Entree. 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 stilles rådighed for databehandler ved login og service-brugen udgør følgende:

- Rolle (fx elev eller lærer)
- Skolekode (institutionsnummer)
- Klassebetegnelse
- Login/hash
- Tekstforståelse: I forbindelse med levering af ydelserne vil oplæsning af den markerede tekst kunne indeholde personoplysninger fra selve teksten.
- Udarbejdelse af tekst: I forbindelse med levering af ydelserne vil teksten indeholde de oplysninger, herunder personoplysninger, som slutbrugeren måtte skrive.
- Tale-til-tekst: I forbindelse med levering af ydelserne, vil selve lydfilen indeholde slutbrugerens stemme, herunder de oplysninger, som slutbrugeren evt. måtte indtale

og oplysninger, som evt. kan udledes af stemmen/lyden, fx oplysninger om køn og sprog.
- Oversættelse: I forbindelse med levering af ydelserne vil den oversatte tekst indeholde de oplysninger, herunder personoplysninger, som slutbrugeren måtte skrive.

Databehandleren behandler som udgangspunkt ikke særlige kategorier af personoplysninger (følsomme personoplysninger, jf. art. 9) under disse Bestemmelser, medmindre den dataansvarlige har givet instruks herom i Aftalen, andre særskilt indgåede aftaler eller tillæg.

Såfremt dataansvarlig eller den dataansvarliges slutbrugere transmitterer eller på anden måde tilgængeliggør særlige kategorier af personoplysninger til eller via databehandleren, herunder dennes underdatabehandlere, hvis omfang bestemmes og kontrolleres af den dataansvarlige, anses dataansvarlig at have givet en instruks til databehandleren om at behandle disse særlige kategorier af personoplysninger i overensstemmelse med disse Bestemmelser.

Det skal bemærkes, at de oplysninger, som slutbrugeren overfører i forbindelse med leveringen af ydelserne, alene opbevares i 7 (syv) dage med henblik på levering af tjenesten samt eventuel support. Herefter slettes disse oplysninger.

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 login.

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

- Rolle (fx medarbejder eller administrator)
- Login/hash
- Tekstforståelse: I forbindelse med levering af ydelserne vil oplæsning af den markerede tekst kunne indeholde personoplysninger fra selve teksten.
- Udarbejdelse af tekst: I forbindelse med levering af ydelserne vil teksten indeholde de oplysninger, herunder personoplysninger, som slutbrugeren måtte skrive.
- Tale-til-tekst: I forbindelse med levering af ydelserne, vil selve lydfilen indeholde slutbrugerens stemme, herunder de oplysninger, som slutbrugeren evt. måtte indtale og oplysninger, som evt. kan udledes af stemmen/lyden, fx oplysninger om køn og sprog.
- Oversættelse: I forbindelse med levering af ydelserne vil den oversatte tekst indeholde de oplysninger, herunder personoplysninger, som slutbrugeren måtte skrive.

Databehandleren behandler som udgangspunkt ikke særlige kategorier af personoplysninger (følsomme personoplysninger, jf. art. 9) under disse Bestemmelser, medmindre den dataansvarlige har givet instruks herom i Aftalen, andre særskilt indgåede aftaler eller tillæg.

Såfremt dataansvarlig eller den dataansvarliges slutbrugere transmitterer eller på anden måde tilgængeliggøre særlige kategorier af personoplysninger til eller via databehandleren, herunder dennes underdatabehandlere, hvis omfang bestemmes og kontrolleres af den dataansvarlige, anses dataansvarlig at have givet en instruks til databehandleren om at behandle disse særlige kategorier af personoplysninger i overensstemmelse med disse Bestemmelser.

Det skal bemærkes, at de oplysninger, som slutbrugeren overfører i forbindelse med leveringen af ydelserne, alene opbevares i 7 (syv) dage med henblik på levering af tjenesten samt eventuel support. Herefter slettes disse oplysninger.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Ansatte tilknyttet dataansvarlige	
Elever/studerende tilknyttet dataansvarlige over 18 år	
Elever/studerende tilknyttet den dataansvarlige under 18 år	
Øvrige registrerede, fx borgere	

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.

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

Europa-Kommissionens standardkontraktbestemmelser (modelklausulerne) for overførsel af personoplysninger til tredjelande etableret uden for EU/EØS (også benævnt "Standard Contractual Clauses"), jf. Europa-Kommissionens gennemførelsesafgørelse 2021/914 af 4. juni 2021 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679, vil i det følgende angives som "Standard Contractual Clauses" eller "SCC".

EU-U.S. Data Privacy Framework, jf. Europa-Kommissionens gennemførelsesafgørelse af 10. Juli 2023 i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679, vil i det følgende angives som "DPF".

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

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING	OVERFØRSELSGRUNDLAG
Amazon Web Services, South Dublin Data Center	N/A	Greenhills Road, Tymon North, Dublin, Ireland	Serverhosting, Oversættelse i online produkter/løsninger	DPF Link til certifikat: https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000TOWQAA4&status=Active
Vitec Software Group, AB	N/A	Göteborg, Sverige	Serverhosting	Ikke relevant
Microsoft Ireland Operations Limited, Microsoft Azure	N/A	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521	Tale-til-tekst behandling i online produkter/løsninger	DPF Link til certifikat: https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active
Abbyy	N/A	Friendenstrasse 22 b, 81671 München, Tyskland	OCR-behandling i online produkter/løsninger	På tidspunktet for Bestemmelsernes indgåelse er overførselsgrundlaget SCC. Såfremt Abbyy i løbet af parternes aftaleforhold certificerer sig under DPF, vil DPF erstatte SCC som overførselsgrundlag.

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

I overensstemmelse med Bestemmelse 7.3, underretter databehandleren den dataansvarlige om eventuelle planlagte ændringer vedrørende de i B.1. ovenfor angivne underdatabehandlere med mindst tredive (30) dages varsel og giver derved den

dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden implementering i forbindelse med udførelsen af tjenesterne på vegne af den dataansvarlige.

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.

C.2. Behandlingssikkerhed

Databehandleren skal gennemføre passende tekniske og organisatoriske kontroller og foranstaltninger for at sikre fortrolighed, integritet og tilgængelighed af de personoplysninger, der behandles på vegne af den dataansvarlige. Personoplysninger skal klassificeres korrekt, og der skal gennemføres passende sikkerhedskontrol på grundlag af denne klassificering.

I forbindelse med leveringen af tjenester på vegne af den dataansvarlige, skal databehandleren som minimum gennemføre følgende sikkerhedskontroller, som er baseret på principperne i ISO27001-standarden og kontrollerne i kontrolmål B vedrørende behandlingssikkerhed i ISAE 3000-erklæringen:

C.2.1. Informationssikkerhedspolitik

C.2.1.1. Databehandleren, herunder dennes leverandører og medarbejdere, skal til enhver tid overholde den interne informationssikkerhedspolitik, der er tilpasset principperne i ISO27001-standarden, som indeholder procedurer, der har til formål at sikre den dataansvarliges data og personoplysninger, så længe de er i databehandlerens varetægt.

C.2.1.2. Databehandleren skal efter at have udført en formel risikovurdering regelmæssigt afprøve interne sikkerhedspolitikker, -planer og -kontroller. Resultatet af ovenstående afprøvning skal kommunikeres til databehandlerens ledelse, og resultater, som direkte påvirker behandlingen af databehandlerens personoplysninger, skal afhjælpes rettidigt.

C.2.1.3. Databehandleren skal vedligeholde og overholde principperne i ISO 27001 eller ISO27701-standarderne for det interne complianceprogram for informationssikkerhedspolitik og databeskyttelse.

C.2.2. Organisering af informationssikkerhed

C.2.2.1. Databehandlerens informationssikkerhedsorganisation skal være organiseret således, at der kan ske effektiv styring og opnåelse af målene for informationssikkerhed.

Ydermere skal databehandleren:

a. fastholde tilstrækkeligt kvalificeret personale med klart definerede roller og ansvarsområder i sin informationssikkerhedsorganisation med henblik på at

koordinere indførelsen af sikkerhedsprocedurer for databehandlerens organisation.
b. fastsætte krav til følsomhed, beskyttelse og videregivelse af oplysninger og hvert år tage sådanne krav op til fornyet vurdering.
c. adskille opgaver, roller og ansvar for at forhindre uautoriseret brug af databehandlerens forretningskritiske informationsaktiver.

C.2.3. HR

C.2.3.1. Baggrundstjek af medarbejdere med adgang til personoplysninger skal være gennemført i henhold til relevant lovgivning, øvrig regulering og etiske krav og skal udføres for hver enkelt person som minimum ved ansættelse, medmindre det er i strid med lovgivningen. Omfanget af baggrundstjek skal være i overensstemmelse med den rolle, den pågældende medarbejder har, følsomhedsgraden af de data, som denne persons rolle vil give adgang til, og de risici, der vil opstå ved misbrug af dataene.

C.2.3.2. Databehandleren skal sikre, at alt personale har underskrevet en fortrolighedsaftale som del af deres ansættelseskontrakt.

C.2.3.3. Databehandleren skal sikre passende awareness og adgang til data, således at databehandlerens brugere forstår deres ansvarsområder i forbindelse med it-sikkerhed for den dataansvarliges data og personoplysninger.

C.2.3.4. Databehandleren skal sikre, at alle nødvendige procedurer udføres for databehandlerens medarbejdere ved skift af rolle, opgaveophør, ophør af ansættelsesforhold, kontrakt eller aftale.

C.2.4. Styring af aktiver

C.2.4.1. Databehandleren skal opretholde procedurer til identifikation, kontrol og opretholdelse af ejerskabs- og sikkerhedsklassificering af nøgleaktiver og den dataansvarliges data og personoplysninger, der opbevares i databehandlerens datacenterinfrastruktur.

C.2.4.2. Databehandleren skal udarbejde politikker for accepteret brug af data og aktiver og kommunikere disse til alle relevante brugere af dens aktiver og data.

C.2.4.3. Databehandleren skal implementere formelle, dokumenterede procedurer for systemhærdning og baseline konfigurering. Ikke-supporteret software eller hardware må ikke anvendes.

C.2.5. Adgangskontrol

C.2.5.1. Databehandleren skal implementere kontroller til sikring af adgangen til personoplysninger, der behandles på vegne af den dataansvarlige.

C.2.5.2. Brugeradgang til de af databehandlerens systemer og applikationer, der lagrer eller giver adgang til personoplysninger, skal kontrolleres gennem en sikker login-procedure.

C.2.5.3. Databehandlerens personale gives adgang til sådanne personoplysninger alt efter arbejdsbehov og princippet om minimering af adgangsrettigheder, idet den enkeltes rolle og ansvar afspejles.

C.2.5.4. Databehandleren skal overvåge og begrænse adgang til hjælpeprogrammer, der kan omgå sikkerhedskontrollerne i systemer eller applikationer. Administrators adgangsrettigheder til end-points skal være begrænset.

C.2.5.5. Adgang til alle databehandlers systemer er sikret med MFA og alle databehandlers medarbejdere med adgang til driftsmiljøer har underskrevet en udvidet fortrolighedserklæring.

C.2.5.6. Den formelle proces for rettidig tilbagekaldelse af adgangen til personoplysninger skal følges, når en person ikke længere har behov for at have adgang til oplysningerne.

C.2.6. Kryptografi

C.2.6.1. Databehandleren skal sikre, at personoplysninger behandlet på vegne af den dataansvarlige beskyttes under opbevaringen og overførslen ved hjælp af stærk kryptering. Denne kryptering skal afspejle almindeligt anerkendte branchestandarder og skal implementeres i overensstemmelse med databehandlerens krypteringsstandard.

C.2.6.2. Leverandøren skal implementere procedurer til styring af krypteringsnøgler, der omfatter:

a. Generering af krypteringsnøgler med godkendt nøglelængde.
b. Sikker distribution, aktivering og lagring, genoprettelse og udskiftning/opdatering af krypteringsnøgler.
c. Øjeblikkelig tilbagekaldelse (deaktivering) af krypteringsnøgler ved kompromittering eller ændring af medarbejderens ansvarsområde.
d. Genoprettelse af krypteringsnøgler, der er forsvundet, beskadiget eller er udløbet.
e. Backup af og arkiv for krypteringsnøgler og vedligeholdelse af historik for krypteringsnøgler.
f. Allokering af tidspunkt for aktivering og deaktivering af definerede krypteringsnøgler.
g. Begrænsning af adgang til krypteringsnøgler til autoriserede personer.

C.2.6.3. Produkterne anvender både kryptering ”in transit” og ”at rest”. Det betyder blandt andet, at alle forbindelser til ”backend” er krypteret med TLS v1.2/v1.3 ”in transit”. Kryptering ”at rest” afhænger af medie, men AES256 er oftest benyttet.

C.2.7. Fysisk sikring og miljøsikring

C.2.7.1. Databehandleren skal gennemføre passende fysiske sikkerhedskontroller med henblik på at sikre fortrolighed, integritet og tilgængelighed af de personoplysninger, der behandles på vegne af den dataansvarlige, på databehandlerens faciliteter, kundelokaliteter eller andre eksterne lokaliteter. Kontrollerne gennemgås regelmæssigt med henblik på at sikre effektiviteten heraf.

C.2.7.2. Databehandleren skal dog – som minimum – gennemføre følgende fysiske sikkerhedsforanstaltninger på sine kontorer:

a. Fysisk adgangskontrol for bygninger og kritiske områder
b. Receptionsområder, der overvåges af receptionistpersonale eller sikkerhedsvagter
c. Logning af fysisk adgang eller forsøg herpå.

C.2.7.3. Som primære driftsmiljø anvendes AWS i Irland, hvor data hostes, og hvor AWS indbyggede CloudTrail er aktiveret. Det betyder, at alle databehandlers medarbejderes logins og handlinger udført i driftsmiljøer bliver logget i 90 dage. Audit-log bliver løbende overvåget.

C.2.8. Driftssikkerhed

C.2.8.1. Databehandleren skal implementere kontroller, der påviser og forhindrer malware, skadelige koder og uautoriseret kørsel af koder. Kontroller skal med jævne mellemrum opdateres med den senest tilgængelige teknologi (fx opdatering af seneste signaturer og definitioner).

C.2.8.2. Databehandleren skal udføre penetrationstest af systemer og applikationer, der lagrer eller giver adgang til personoplysninger.

C.2.8.3. Databehandleren skal implementere en proces for håndtering af opdateringer og sårbarheder for systemer og applikationer til identifikation, rapportering og afhjælpning af sårbarheder.

C.2.8.4. Databehandleren skal generere administrator- og hændelseslogs for systemer og applikationer, der lagrer eller giver adgang til personoplysninger.

C.2.8.5. Databehandleren skal med jævne mellemrum gennemgå systemlogs (mindst én gang om måneden) for at identificere systemudfald, fejl eller mulige sikkerhedshændelser, der påvirker personoplysningerne. Afhjælpning af fejl skal foretages for at løse eller tage hånd om forhold inden for den nødvendige tidshorisont.

C.2.9. Kommunikationssikkerhed

C.2.9.1. Databehandleren skal etablere en sikker VPN-forbindelse (Virtual Private Network), som medarbejderne skal benytte ved fjernadgang til databehandlerens interne netværk. Brugere skal benytte to-faktorgodkendelse for at få adgang via VPN-forbindelsen.

C.2.9.2. Databehandleren skal anvende avancerede firewalls til beskyttelse af sit netværk, herunder beskyttelse mod skadelig software og avanceret indtrængning i netværket, samt til segmentering af netværket for at sikre dets robusthed.

C.2.9.3. Databehandleren skal implementere løsninger, der er udformet til at overvåge og logge aktiviteten på sit netværk. Loggen skal overvåges løbende for rettidigt at kunne identificere og løse sikkerhedshændelser, og den skal opbevares i overensstemmelse med databehandlerens formelle politikker og procedurer.

C.2.9.4. Databehandleren skal synkronisere systemure på netværksservere til en universaltid (fx UTC) eller til network time protocol (NTP).

C.2.10. Anskaffelse, udvikling og vedligeholdelse af systemer

C.2.10.1. Databehandlerens indkøbsproces for hardware, software og tjenesteydelser skal dokumenteres og omfatte identifikation og vurdering af it-sikkerhedsrisici.

C.2.10.2. Databehandleren skal implementere formelle, dokumenterede procedurer til styring af ændringer i informationssystemer, understøttende infrastruktur og faciliteter.

C.2.10.3. Databehandleren skal etablere en logisk eller fysisk adskillelse i systemmiljø af udvikling, test og produktion. Brugeradgang til kildekode til programmer skal begrænses og registreres.

C.2.10.4. Databehandlerens skal etablere en sikker fremgangsmåde for systemkonstruktion og kodning, der dokumenteres og integreres i systemudviklingens livscyklus (SDLC). Udviklere skal med jævne mellemrum deltage i kurser om sikker udvikling.

C.2.10.5. Databehandlerens ændringer i systemer og applikationer skal testes og opfylde fastlagte godkendelseskriterier forud for implementeringen heraf. Tests skal omfatte de relevante sikkerhedskontroller.

C.2.10.6. Databehandlerens produktionsdata må ikke bruges i andre miljøer end produktionsmiljøet. Hvis sådan brug er uundgåelig, skal data maskeres (fx sløres, renses, pseudonymiseres, anonymiseres), eller der skal indføres sikkerhedskontroller svarende til dem, der findes i produktionsmiljøet, for de øvrige miljøer.

C.2.10.7. Der skal gennemføres automatiseret, statisk kildekodeanalyse og afhjælpning af sårbarheder for databehandlerens kildekode forud for implementering.

C.2.10.8. Databehandleren skal overvåge outsourcet systemudvikling, der er underlagt styringskontrol hos ekstern leverandør.

C.2.11. Styring af leverandørforhold

C.2.11.1. Databehandleren skal udarbejde og opretholde formelle aftaler med de leverandører, der er involveret i styringen af serviceydelser vedrørende databehandlerens informationssystemer, og hvor relevant inkorporere de nødvendige sikkerhedskontroller, -politikker og serviceaftaler.

C.2.11.2. Databehandleren skal med jævne mellemrum gennemgå sine eksterne parters it-sikkerhedskontroller og kontrollere, at disse kontroller fortsat er relevante i forhold til de risici, der er forbundet med de eksterne parters behandling af personoplysninger, samtidig med at der tages højde for det tekniske niveau og implementeringsomkostningerne.

C.2.11.3. Databehandleren skal begrænse eksterne parters adgang til personoplysninger. Når der er behov for adgang til data for at kunne opfylde aftalen om levering af ydelser, skal databehandleren:

a. give den dataansvarlige en oversigt over de eksterne parter, der har behov for adgang til personoplysninger
b. kun give tilladelse til at tilgå personoplysninger, når det er nødvendigt for levering af de ydelser, som den eksterne part har indgået aftale om at levere
c. registrere den eksterne parts adgang til personoplysninger, i systemlogs, der er omfattet af databehandlerens kontrol af registrering og overvågning.

C.2.12. Styring af informationssikkerhedshændelser

C.2.12.1. Databehandleren skal udarbejde og vedligeholde en hændelsesberedskabsplan og et program, der indeholder procedurer og anvisninger, der skal følges i tilfælde af en hændelse relateret til databehandlerens computerinfrastruktur, og de nødvendige skridt og kommunikationskanaler, der skal følges, skal dokumenteres.

C.2.12.2. Databehandleren skal sikre, at anvisningerne omfatter passende procedurer for øjeblikkelig underretning af databehandlerens kunder og andre nødvendige interessenter, hvis

det fastslås, at en sikkerhedshændelse har forårsaget et sikkerhedsbrud, der involverer personoplysninger.

C.2.13. Informationssikkerhedsaspekter ved nød- beredskabs- og reetableringsstyring

C.2.13.1. Databehandleren skal have en plan for forretningskontinuitet/katastrofeberedskab, som skal anvendes til rettidig gendannelse af databehandlerens kritiske systemer, applikationer og komponenter i tilfælde af en fysisk eller teknisk hændelse.

C.2.13.2. Databehandleren skal afprøve ovennævnte planer regelmæssigt/årligt og sørge for, at de er opdateret.

C.2.13.3 Databehandleren skal indføre procedurer til identifikation og validering af backup, der er nødvendige som understøttelse af katastrofeberedskabet.

C.2.13.4 Databehandleren skal sørge for passende opbevaring af backup til sikring af katastrofeberedskabet og implementere hensigtsmæssige bortskaffelsesprocedurer, der overholder opbevaringskravene.

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 alle 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 den dataansvarlige anmoder UNI-C om at identificere den pågældende bruger og dermed gøre databehandler i stand til at fremfinde og slette data.

Erhvervskunder

Brugeren kan identificeres ved hjælp af f.eks. e-mailadresse og 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.

Bemærk, at oplysninger, som fremkommer i forbindelse med leveringen af ydelserne, slettes efter 7 (syv) dage, jf. pkt. A.3.

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:

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

Herudover kan behandlingen til enhver tid ske på de lokaliteter, hvor databehandlerens medarbejdere har hjemmearbejdspladser og lignende.

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

NAVN	ADRESSE	PLACERING AF DATACENTER	GEOFRAFISK LOKATION AF MODERSELSKAB
Amazon Web Services Inc., South Dublin Data Center ("AWS")	Greenhills Road, Tymon North, Dublin, Ireland	Personoplysninger opbevares i AWS' datacenter i Dublin.	USA
Vitec Software Group, Koncern IT	Göteborg, Sverige	Sverige	Sverige
Microsoft Ireland Operations Limited, Microsoft Azure ("Microsoft")	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521	Personoplysninger opbevares i Microsofts datacenter i Nordeuropa	USA
Abbyy	Friendenstrasse 22 b, 81671 München, Tyskland	Personoplysninger opbevares i Microsofts datacenter i Den europæiske Union	USA

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 overfører, som led i sin behandling af personoplysninger på vegne af den dataansvarlige personoplysninger til USA. Retsgrundlaget for overførslen til USA er EU-U.S. Data Privacy Framework (DPF), jf. Europa-Kommissionens gennemførelsesafgørelse af 10. Juli 2023 i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679, jf. de i skema B.1. nævnte databehandlere. Ved Bestemmelsernes ikrafttræden har EU-Kommissionen truffet en tilstrækkelighedsafgørelse på baggrund af EU-U.S. Data Privacy Framework (DPF), som udgør et lovligt overførselsgrundlag.

I tilfælde af, at DPF ophører, eller på anden vis ugyldiggøres som overførselsgrundlag, vil Standard Contractual Clauses finde anvendelse i stedet for.

For så vidt angår underdatabehandleren "Abbyy", som er angivet under afsnit B.1., er denne underdatabehandler ved Bestemmelsernes ikrafttræden ikke certificeret under DPF. Retsgrundlaget for overførslen af personoplysninger til Abbyy er Standard Contractual Clauses.

Såfremt Abbyy på et tidspunkt i løbet af Bestemmelsernes varighed bliver certificeret under DPF, vil retsgrundlaget for overførsel af personoplysninger til USA, der involverer Abbyy, overgå til at være DPF.

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 enhver anden erklæring baseret på sammenlignelige eller strengere standarder.

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.

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

Databehandleren skal én gang årligt for underdatabehandlerens regning indhente en revisionserklæring fra en uafhængig ekstern part vedrørende de sikkerhedsforanstaltninger, underdatabehandleren har implementeret i forbindelse med 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, Soc 1 og Soc 2, type I eller type II, eller enhver anden erklæring baseret på sammenlignelige eller strengere standarder, eller tilsyn baseret på databehandlerens egne krav til eksterne leverandørers behandlings- og informationssikkerhedspolitik.

Hvis underdatabehandleren er ISO 27001- eller ISO 27701-certificeret i Bestemmelsernes løbetid, betragtes certificeringen – eventuelt suppleret med ledelseserklæringer mv. - som værende passende tilsyn.

Databehandleren skal på den dataansvarliges skriftlige anmodning underrette underdatabehandleren om, uden unødig forsinkelse, at fremsende revisionserklæring, ISO 27001- eller ISO 27701-certifikat, alt efter relevans.

Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til databehandlere og underdatabehandlere kan til enhver tid ske med udgangspunkt i den tilsynsform, som findes at være passende i overensstemmelse med Datatilsynets "Vejledning om tilsyn med databehandlere".

Bilag D Parternes regulering af andre forhold

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.

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, 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.