Changelog

VERSION	ÆNDRINGER
1.1	Ændringer i Bestemmelserne 7.7., 9.2., 10.4. og Bilag C.8. *(Tastefejl og opdaterede krydshenvisninger).*
1.2	Ændringer i Bestemmelse 7.6 *(Bestemmelsen er gjort valgfri og ordlyden er blevet modificeret)*

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

mellem

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

herefter ”den dataansvarlige”

og

opgaveforsvar.dk v/Njal Laursen Würtz
CVR 46696891
Bygholm Parkvej 57
8700 Horsens
Danmark

herefter ”databehandleren”

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

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

1. Indhold

2. Præambel 4
3. Den dataansvarliges rettigheder og forpligtelser 4
4. Databehandleren handler efter instruks 5
5. Fortrolighed 5
6. Behandlingssikkerhed 5
7. Anvendelse af underdatabehandlere 6
8. Overførsel til tredjelande eller internationale organisationer 7
9. Bistand til den dataansvarlige 8
10. Underretning om brud på persondatasikkerheden 9
11. Sletning og returnering af oplysninger 9
12. Revision, herunder inspektion 9
13. Parternes aftale om andre forhold 10
14. Ikrafttræden og ophør 10
15. Kontaktpersoner hos den dataansvarlige og databehandleren 11
Bilag A Oplysninger om behandlingen 12
Bilag B Underdatabehandlere 15
Bilag C Instruks vedrørende behandling af personoplysninger 16
Bilag D Parternes regulering af andre forhold 20

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 opgaveforsvar.dk 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.

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.

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.

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 nærmeret angivet i Bilag C.7. og C.8.

3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

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

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft 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 skriftlig 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	Njal Laursen Würtz
Stilling	Indehaver, opgaveforsvar.dk
Telefonnummer	+45 28 78 14 33
E-mail	njal@opgaveforsvar.dk

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	Njal Laursen Würtz
Stilling	Indehaver, opgaveforsvar.dk
Telefonnummer	+45 28 78 14 33
E-mail	njal@opgaveforsvar.dk

Bilag A Oplysninger om behandlingen

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

Formålet med behandlingen er:

- at stille webtjenesten opgaveforsvar.dk til rådighed for den dataansvarlige institution
- at understøtte læreres egen planlægning, evaluering og feedback på elevers skriftlige arbejde
- at lade elever gennemføre en AI-baseret skriftlig samtale om deres egen opgave
- at lade elever gennemføre en kort skriftlig Exit-samtale ved timens afslutning om lærerens læringsmål og kernespørgsmål
- at give læreren adgang til struktureret dokumentation af de spørgsmål eleven fik, elevens faktiske svar og relevante tekststeder som grundlag for lærerens egen faglige vurdering
- at give læreren adgang til faktuelle deltagelses- og sessionsoplysninger samt ordrette samtaleturns fra Exit-samtaler
- at understøtte undervisning, lærerens egen evaluering, feedback og faglig refleksion
- at sikre drift, sikkerhed, support og fejlretning af tjenesten. Videreudvikling af tjenesten må kun ske på anonymiserede, aggregerede eller på anden måde ikke-personhenførbare oplysninger, medmindre den dataansvarlige har givet særskilt dokumenteret instruks.

Præcisering: opgaveforsvar.dk foretager ikke faglig vurdering, scoring eller klassifikation af elevens faglige niveau og anvendes ikke til automatisk karaktergivning. Tjenesten stiller spørgsmål og dokumenterer elevens svar; den faglige vurdering foretages af den dataansvarliges personale. Læreren har det fulde ansvar for enhver pædagogisk, faglig eller administrativ opfølgning.

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

Behandlingen på vegne af den dataansvarlige drejer sig primært om:

- indsamling af oplysninger fra lærere og elever ved oprettelse, login og brug af tjenesten
- registrering og opbevaring af opgavebeskrivelser, klasse-/holdoplysninger og elevbidrag
- modtagelse og behandling af elevens uploadede opgave (PDF, DOCX m.v.)
- tekstudtræk fra uploadede dokumenter
- server-side regelbaseret maskering og dataminimering af elevtekst, transcript og opgavekontekst (deterministisk regex-baseret erstatning af udvalgte direkte identifikatorer såsom CPR, e-mail, telefonnumre, ID-numre, URL'er og sociale profiler) inden tekst sendes til AI-tjeneste i opgaveforsvarsflowet
- automatiseret teknisk indholdskontrol med henblik på at identificere klart upassende eller åbenbart ikke-anvendeligt input
- generering af AI-baserede spørgsmål og opfølgning gennem en skriftlig samtale med eleven
- behandling og lagring af elevens skriftlige svar samt deterministisk strukturering af spørgsmål, svar, relevante tekststeder og administrative gennemførelsesoplysninger i et struktureret dokumentationspost
- gennemførelse af Exit-samtaler: registrering af lærerens konfiguration (læringsmål, kernespørgsmål og materiale), behandling af elevens korte skriftlige svar og, hvor den adaptive funktion er aktiveret, et internt afgrænset AI-baseret styringssignal, der alene kan anvendes til valg af næste neutrale opfølgende spørgsmål eller samtalens videre forløb. Styringssignalet vises ikke som lærer- eller elevrettet faglig vurdering

- visning af ordrette spørgsmål, elevsvar, samtaleturns og faktuelle deltagelses-/sessionsoplysninger til læreren
- strukturering, visning og søgning i ovenstående oplysninger i lærerens dashboard
- adgangsstyring, autentifikation og logning af relevante hændelser
- sletning af oplysninger efter aftalte sletteregler eller dokumenteret instruks

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

Behandlingen omfatter følgende typer af almindelige personoplysninger, jf. databeskyttelsesforordningens artikel 6:

- Lærerens navn, e-mailadresse og loginoplysninger (krypteret/hashet adgangskode)
- Skole-/institutionsoplysninger og klasse-/holdoplysninger oprettet af læreren
- Opgavetitel, opgavebeskrivelse og fagligt kontekstmateriale tilføjet af læreren
- Elevens fornavn, pseudonym eller andet identifikationsfelt, hvis dette indtastes af eleven eller fremgår af det uploadede materiale
- Elevens skriftlige opgave/besvarelse (fritekst), herunder eventuelt indhold ekstraheret fra elevens uploadede dokumenter
- Elevens skriftlige svar i den AI-baserede samtale
- Elevens korte skriftlige svar i Exit-samtaler samt en valgfri, lærerindtastet deltagerliste med elevfornavne; elevens session identificeres ved en tilfældig token, der alene gemmes som SHA-256-hash
- AI-genererede spørgsmål samt strukturerede struktureret dokumentationsposts med spørgsmål, ordrette elevsvar, relevante tekststeder og administrative metadata
- Interne tekniske/adaptive metadata knyttet til Exit-svar, hvor sådanne metadata behandles alene for at styre næste spørgsmål og ikke vises som en faglig vurdering af eleven
- Lærerens kommentarer eller feedback i tjenesten, hvor sådanne funktioner er tilgængelige
- Tekniske metadata, systemlogs, tidsstempler og sessionsoplysninger, herunder fejl- og sikkerhedslogs, IP-adresser, user agent, browser-/enhedsoplysninger, request-tidsstempler og tekniske fejldata i det omfang disse behandles af applikationen eller underdatabehandlere

Præcisering vedrørende artikel 9 og 10:

- Tjenesten er ikke beregnet til behandling af særlige kategorier af personoplysninger, jf. databeskyttelsesforordningens artikel 9, eller oplysninger om strafbare forhold, jf. forordningens artikel 10.
- Sådanne oplysninger må ikke uploades eller indtastes i tjenesten, medmindre den dataansvarlige har et selvstændigt behandlingsgrundlag og har givet databehandleren skriftlig dokumenteret instruks herom.
- Da dele af behandlingen omfatter fritekst fra elever, kan sådanne oplysninger forekomme utilsigtet. Databehandleren anvender tekniske og organisatoriske foranstaltninger for at reducere risikoen, herunder server-side regelbaseret maskering og dataminimering af elevtekst, transcript og opgavekontekst inden AI-behandling samt teknisk indholdskontrol. Maskeringen er designet til at fjerne udvalgte direkte identifikatorer (CPR, e-mail, telefon, ID-numre, URL'er og sociale profiler) inden videregivelse til Azure.
- Hvis utilsigtet forekomst af særlige kategorier eller artikel 10-oplysninger identificeres, håndteres de efter den dataansvarliges instruks, herunder ved sletning eller blokering.

A.4. Behandlingen omfatter følgende kategorier af registrerede

- Elever og kursister ved den dataansvarlige institution
- Lærere og eventuelle administrative brugere ved den dataansvarlige institution

- Eventuelle kontaktpersoner hos den dataansvarlige, der oprettes eller tildeles adgang til tjenesten

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

- Behandlingen påbegyndes ved Bestemmelsernes ikrafttræden.
- Behandlingen varer, så længe den dataansvarlige anvender tjenesten.
- Interviewdata (samtaler, transcripts, struktureret dokumentationsposts og tilhørende metadata) slettes automatisk senest 90 dage efter samtalens tidsstempel, jf. den tekniske håndhævelse beskrevet i Bilag C.4.
- Historiske interviewdata, der er oprettet før overgangen til den nuværende dokumentationsbaserede løsning, kan frem til sletning efter den samme 90-dages opbevaringsperiode indeholde ældre afledte AI-vurderingsdata. Den nuværende opgaveforsvarsløsning opretter eller eksponerer ikke sådanne faglige AI-vurderinger.
- Exit-samtaledata (deltagerliste med fornavne, elevsvar, interne adaptive metadata og dokumentations-/resultatdata) slettes automatisk senest 90 dage efter samtalen via en særskilt daglig sletterutine; lærerens konfiguration bevares uden elevliste, jf. Bilag C.4.
- Lærer- og kontooplysninger samt opgavedefinitioner opbevares, så længe lærerens konto er aktiv.
- Ved ophør af tjenesten slettes aktive personoplysninger senest 30 dage efter ophør eller efter den dataansvarliges dokumenterede instruks, medmindre lovgivning kræver længere opbevaring. Eventuelle tekniske backupkopier håndteres som beskrevet nedenfor og i Bilag C.4.
- Backupkopier og deres opbevaringsperiode følger de godkendte underdatabehandleres dokumenterede backup-, gendannelses- og opbevaringsvilkår. Eventuelle personoplysninger, der alene består i backupkopier, er fortsat omfattet af disse Bestemmelser, indtil de er overskrevet eller slettet efter den pågældende leverandørs dokumenterede backupcyklus.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Supabase Inc.	Ikke relevant	970 Toa Payoh North #07-04, Singapore 318992.	Hosting af relationel database (PostgreSQL), autentifikation samt lagring af lærerkonti, opgaver, interviewdata, transcripts, strukturerede dokumentationsposter, Exit-data og tekniske logs. Projektets primære region er konfigureret til Frankfurt, Tyskland.
Vercel Inc.	Ikke relevant	440 N Barranca Avenue #4133, Covina, CA 91723, USA.	Hosting af web-applikationen opgaveforsvar.dk (Next.js), HTTPS, statiske aktiver og serverfunktioner samt planlagte server-side jobs. Det aktuelle produktionsmiljø er konfigureret til Stockholm, Sverige (Vercel-region arn1).
Microsoft Ireland Operations Limited (Microsoft Azure OpenAI Service)	Ikke relevant	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland.	AI-baseret generering og tilpasning af spørgsmål, afgrænset teknisk indholdskontrol og intern adaptiv styring af næste neutrale spørgsmål. Tjenesten anvendes ikke til lærer- eller elevrettede faglige vurderinger efter et opgaveforsvar. Azure OpenAI er konfigureret som EU Data Zone Standard.
Plus Five Five, Inc. d/b/a Resend	Ikke relevant	2261 Market Street #5039, San Francisco, CA 94114, USA.	Udsendelse af transaktionelle systemmails til lærer-/administrative brugere. Anvendes ikke til at sende elevoplysninger eller samtaleindhold.

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

B.2. Varsel for godkendelse af underdatabehandlere

Databehandleren skal med mindst 30 dages skriftligt varsel underrette den dataansvarlige om planlagte tilføjelser eller udskiftninger af underdatabehandlere. Den dataansvarlige kan inden ændringen træder i kraft gøre skriftlig indsigelse. Hvis indsigelsen ikke kan imødekommes, kan parterne opsige aftalen om den berørte behandlingsaktivitet. Hvis en ændring undtagelsesvis er nødvendig af akutte sikkerheds- eller driftsmæssige årsager, kan databehandleren gennemføre ændringen hurtigere, men skal orientere den dataansvarlige uden unødig forsinkelse og skriftligt redegøre for nødvendigheden. Underretning sker pr. e-mail til den i pkt. 15 angivne kontaktperson hos 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:

Databehandleren må alene behandle personoplysninger med henblik på at levere, drifte, sikre, supportere og fejlrette opgaveforsvar.dk for den dataansvarlige, herunder:

- oprettelse og administration af lærerbrugere og adgangsroller
- oprettelse af opgaver, klasser/hold og adgangskoder/links til elever
- modtagelse og behandling af elevens uploadede opgave
- tekstudtræk fra uploadede dokumenter
- server-side regelbaseret maskering og dataminimering af elevtekst, transcript og opgavekontekst før relevante AI-behandlinger i opgaveforsvarsflowet og i andre flows, hvor den dokumenterede maskeringsfunktion anvendes
- teknisk indholdskontrol med henblik på at identificere klart upassende eller åbenbart ikke-anvendeligt input
- generering af AI-baserede spørgsmål og opfølgning
- modtagelse, lagring og deterministisk strukturering af elevens skriftlige svar i et struktureret dokumentationspost
- visning af spørgsmål, ordrette elevsvar, relevante tekststeder, transcripts samt faktuelle deltagelses- og sessionsoplysninger til læreren
- internt afgrænset Exit-styringssignal, hvis og kun hvis den adaptive funktion er aktiveret, og signalet alene anvendes til at styre næste neutrale spørgsmål eller samtalens videre forløb og ikke eksponeres som en faglig vurdering af eleven
- fejlfinding, sikkerhedsovervågning, logning og support i nødvendigt omfang
- automatisk sletning af interview- og Exit-samtaledata efter 90 dage og sletning/eksport efter aftale eller dokumenteret instruks

Tjenesten foretager ikke faglig vurdering, scoring eller klassifikation af elevens faglige niveau og anvendes ikke til automatisk karaktergivning. AI anvendes til at stille og eventuelt tilpasse spørgsmål; den faglige vurdering af elevens svar foretages af den dataansvarliges personale.

Databehandleren må ikke:

- anvende personoplysninger til egne formål ud over levering af tjenesten
- anvende personoplysninger til træning af generelle AI-modeller eller grundmodeller
- anvende personoplysninger til videreudvikling af tjenesten i identificerbar form. Videreudvikling må alene ske på anonymiserede, aggregerede eller på anden måde ikke-personhenførbare oplysninger, medmindre den dataansvarlige har givet særskilt dokumenteret instruks
- videregive personoplysninger til andre end de godkendte underdatabehandlere, jf. Bilag B, eller ud over hvad der følger af dokumenteret instruks eller lov
- behandle personoplysninger til andre formål end dem, der er fastlagt i denne aftale og dens bilag

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Risikovurdering: Behandlingen omfatter almindelige personoplysninger om elever og lærere, elevopgaver og samtalesvar i fritekst, som kan indeholde personligt eller fagligt følsomt indhold. Tjenesten er ikke beregnet til artikel 9- eller artikel 10-oplysninger, men sådanne oplysninger kan forekomme utilsigtet i fritekst. Behandlingen indebærer overførsel af tekst til en AI-

underdatabehandler i de flows, der genererer eller tilpasser spørgsmål eller udfører den dokumenterede tekniske indholdskontrol. Sikkerhedsniveauet skal derfor mindst svare til middel og på visse punkter forhøjet sikkerhed.

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:

Pseudonymisering og kryptering: Personoplysninger krypteres under transport via HTTPS/TLS og i hvile hos relevante cloud-underdatabehandlere i overensstemmelse med deres standardvilkår. I de almindelige opgaveforsvarsflows udføres server-side regelbaseret maskering af CPR, e-mail, telefonnumre, ID-numre, URL'er og sociale profiler før videregivelse til AI-underdatabehandler.

Fortrolighed, integritet, tilgængelighed og robusthed: Der anvendes adgangsstyring og rollebaseret adgangskontrol, herunder Row Level Security, logisk kundeadskillelse, begrænset administratoradgang, fortrolighedsforpligtelser, inputbegrænsninger samt sikker udviklingspraksis med versionsstyring, code review og kontrolleret deployment.

Genoprettelse: Backup og gendannelse følger de anvendte underdatabehandleres dokumenterede backup-, gendannelses- og opbevaringsvilkår. Databehandleren skal sikre, at de valgte leverandørers tilgængelige gendannelsesmekanismer indgår i den løbende vurdering af tjenestens robusthed og mulighed for genoprettelse.

Regelmæssig afprøvning og evaluering: Adgange og sikkerhedsforanstaltninger gennemgås periodisk. Sikker udviklingspraksis, code review, kontrolleret deployment og leverandørernes tilgængelige sikkerheds- og compliance-dokumentation indgår i den løbende vurdering.

Adgang via internettet: Adgang til tjenesten sker via HTTPS/TLS med autentifikation, rollebaseret adgang og logisk segmentering, så lærere og institutioner alene kan tilgå egne data.

Beskyttelse under transmission: Data transmitteres over HTTPS/TLS. Før videregivelse til Azure OpenAI i de almindelige opgaveforsvarsflows udføres server-side regelbaseret maskering og dataminimering af udvalgte direkte identifikatorer.

Beskyttelse under opbevaring: Relevante cloud-underdatabehandlere anvender kryptering i hvile efter deres standardvilkår. Databaseadgang er begrænset via adgangskontrol og Row Level Security, og personoplysninger opbevares efter de fastlagte sletteregler i Bilag C.4.

Fysisk sikring: Fysisk sikring af cloudlokaliteter følger de godkendte underdatabehandleres dokumenterede sikkerhedsforanstaltninger. Databehandlerens egen adgang til produktionsdata er begrænset til personer, hvor adgang er nødvendig for drift, support eller fejlfinding.

Hjemme-/fjernarbejdspladser: Kravene til adgangsbegrænsning, fortrolighed, nødvendighed og krypteret transmission gælder uanset arbejdssted. Adgang til produktionsdata må kun ske i det omfang, det er nødvendigt for drift, support eller fejlfinding, og via adgangskontrollerede konti og systemer.

Logning: Applikationslogning i relevante AI- og afslutningsflows er indrettet, så elevtekst, prompts, transcripts og rå modeloutput ikke logges som almindelige driftslogs. Resterende

drifts- og sikkerhedslogs indeholder primært tekniske metadata. Samtaletranscripts og strukturerede dokumentationsposter lagres i databasen inden for den aftalte opbevaringsperiode, så læreren kan se den autentiske samtale i sit dashboard.

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:

Databehandleren bistår den dataansvarlige uden unødig forsinkelse og så vidt muligt inden for de frister, som lovgivningen og den konkrete situation tilsiger. Bistand, der går væsentligt ud over almindelig drift af tjenesten, kan afregnes efter forudgående skriftlig aftale.

- besvarelse af henvendelser fra registrerede vedrørende indsigt, berigtigelse, sletning, begrænsning af behandling og indsigelse
- eksport eller udlevering af personoplysninger om en bestemt registreret i et almindeligt læsbart format, i det omfang systemet understøtter dette
- information og dokumentation om underdatabehandlere, dataplaceringer og overførselsgrundlag
- information om de tekniske og organisatoriske sikkerhedsforanstaltninger med henblik på den dataansvarliges DPIA og overholdelse af artikel 32
- håndtering og underretning ved brud på persondatasikkerheden i overensstemmelse med pkt. 10 og C.2
- relevant dokumentation til brug for den dataansvarliges samarbejde med Datatilsynet
- ved brud på persondatasikkerheden: karakteren og omfanget af bruddet, kategorier og omtrentligt antal berørte registrerede og registreringer, berørte datakategorier, sandsynlige konsekvenser, afhjælpende foranstaltninger samt kontaktpunkt hos databehandleren

C.4 Opbevaringsperiode/sletterutine

- Elevens uploadede fil opbevares ikke varigt som en selvstændig filkopi. Udtrukket opgavetekst anvendes forbigående til at gennemføre opgaveforsvaret. De oplysninger, der bevares efter samtalen, er de aftalte interviewdata og dokumentationsoplysninger beskrevet nedenfor.
- Interviewdata (samtaletranscripts, strukturerede dokumentationsposter, elevens fornavn/pseudonym samt tilhørende metadata) slettes automatisk senest 90 dage efter samtalens tidsstempel.
- Historiske interviewdata fra før overgangen til den nuværende dokumentationsbaserede løsning kan frem til samme slettefrist indeholde ældre afledte AI-vurderingsdata. Den nuværende tjeneste opretter ikke sådanne faglige AI-vurderinger.
- Exit-samtaledata (deltagerliste med fornavne, elevsvar, interne adaptive styringsmetadata og dokumentationsdata) slettes automatisk senest 90 dage efter samtalen. Lærerens konfiguration kan bevares uden elevliste og elevsvar, så længe den relevante lærer-/kontoopsætning er aktiv.
- De automatiske sletterutiner køres server-side og er adgangsbegrænsede. De konkrete jobnavne, køretider og tekniske implementeringsdetaljer kan ændres, uden at de aftalte maksimale slettefrister forlænges.
- Lærer- og kontooplysninger samt opgavedefinitioner opbevares, så længe lærerens konto er aktiv, eller indtil den dataansvarlige giver dokumenteret instruks om tidligere sletning.
- Systemlogs opbevares kun så længe, det er nødvendigt af hensyn til drift, sikkerhed og fejlfinding.

- Den dataansvarlige kan på ethvert tidspunkt anmode om tidligere sletning af specifikke samtaler, opgaver eller personoplysninger for institutionen, i det omfang sletningen ikke strider mod dokumenteret instruks eller lovgivning.
- Ved ophør af tjenesten slettes aktive personoplysninger senest 30 dage efter ophør eller efter den dataansvarliges dokumenterede instruks, jf. Bestemmelse 11.1. Eventuelle personoplysninger, der herefter alene består i tekniske backupkopier, forbliver beskyttet efter disse Bestemmelser og overskrives eller slettes efter den relevante underdatabehandlers dokumenterede backup- og opbevaringscyklus.

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:

- Databehandlerens egen behandling: Danmark/EU/EØS.
- Supabase: primært EU (Frankfurt, Tyskland) som konfigureret i cloudopsætningen. Supportadgang kan ske fra USA, jf. Bilag B.
- Microsoft Azure OpenAI: ressourcen er oprettet i EU (Sweden Central, Sverige), og det anvendte deployment er af typen Data Zone Standard for EU. Behandling af prompts og svar kan ske i Azure-lokationer i EU-medlemsstater inden for Microsofts EU-datazone og ikke udelukkende i Sverige. Data i hvile forbliver i den udpegede Azure-geografi. Eventuel supportadgang er omfattet af Microsofts standardvilkår og overførselsgrundlag, jf. Bilag B.
- Vercel: Det aktuelle produktionsmiljø er konfigureret til Stockholm, Sverige (Vercel-region arn1). Platform, support, logs, build og administrativ behandling kan ske uden for Danmark/EU, jf. Bilag B.
- Resend: levering af e-mailtjeneste kan ske fra USA, jf. Bilag B.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Den dataansvarlige instruerer databehandleren i at gennemføre behandlingen primært inden for EU/EØS, men anerkender og instruerer i, at behandling i begrænset omfang kan medføre overførsel af personoplysninger til tredjeland (USA) i forbindelse med:
- supportadgang og drift hos Supabase Inc.
- hosting, drift og support hos Vercel Inc.
- supportadgang hos Microsoft i tilknytning til Azure OpenAI Service
- levering af e-mailtjeneste fra Plus Five Five, Inc. d/b/a Resend

Overførselsgrundlaget er EU-Kommissionens standardkontraktbestemmelser (SCC) i henhold til afgørelse (EU) 2021/914 indgået med de i Bilag B angivne underdatabehandlere som en del af deres respektive databehandleraftaler/Data Processing Addenda. Hvor den konkrete underdatabehandler eller relevante amerikanske modtagerenhed er certificeret under EU-US Data Privacy Framework (DPF), kan overførsler tillige ske på dette grundlag. DPF angives kun, hvor certificeringen kan dokumenteres. Supplerende foranstaltninger omfatter kryptering under transport og i hvile, adgangsbegrænsninger, dataminimering, server-side maskering før AI-behandling samt aftalte databehandlingsforpligtelser.
Præcisering: Behandling af prompts og svar i Microsofts EU-datazone, jf. Bilag B og C.5, sker inden for EU/EØS og udgør ikke i sig selv en overførsel til tredjeland. Ændringer i underdatabehandlere, dataplacering eller supportadgang, der indebærer en ny tredjelandsoverførsel, kræver opdatering af Bilag B og Bilag C samt etablering af et relevant overførselsgrundlag.

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

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

Den dataansvarlige kan én gang årligt og ud over dette i tilfælde af konkret saglig anledning anmode om dokumentation, der kan påvise databehandlerens overholdelse af databeskyttelsesforordningens artikel 28 og disse Bestemmelser.

- Databehandleren stiller relevant dokumentation til rådighed, herunder beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger, opdateret underdatabehandlerliste, kopi af underdatabehandleraftaler/DPA'er efter anmodning, samt foreliggende revisionserklæringer, certificeringer og sikkerhedsdokumentation fra underdatabehandlere (fx ISO 27001, SOC 2, ISAE 3402) i det omfang databehandleren har adgang til denne dokumentation.
- Den dataansvarlige eller en bemyndiget revisor kan med rimeligt skriftligt varsel og efter saglig begrundelse foretage en fysisk eller fjern-baseret inspektion af de dele af databehandlerens organisation og systemer, der vedrører behandlingen for den dataansvarlige.
- Inspektioner skal gennemføres på en måde, der ikke kompromitterer andre kunders data, forretningshemmeligheder eller sikkerhed, og inden for almindelig arbejdstid.
- Den dataansvarliges egne udgifter ved inspektioner afholdes af den dataansvarlige selv. Databehandlerens medvirken i normalt omfang er omfattet af de aftalte vilkår, mens væsentlig medgået tid kan afregnes efter forudgående aftale.
- Resultatet af en revision/inspektion stilles til rådighed for den dataansvarlige, og den dataansvarlige kan på baggrund af resultatet anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelse af forordningen og disse Bestemmelser.
- Tilsynsmyndigheders adgang i henhold til lovgivningen, jf. Bestemmelse 12.3, påvirkes ikke.

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

Databehandleren fører tilsyn med underdatabehandlere via deres databehandleraftaler/DPA'er, sikkerhedsdokumentation, certificeringer (fx ISO 27001, SOC 2, ISAE 3402) og offentliggjort compliance-dokumentation.

- Databehandleren stiller sådan dokumentation til rådighed for den dataansvarlige i det omfang dokumentationen er tilgængelig og kan deles.
- Databehandleren reagerer på væsentlige ændringer i en underdatabehandlers sikkerheds- eller compliance-forhold, herunder ved at vurdere fortsat anvendelse, kræve afhjælpning eller udskifte underdatabehandleren.
- Den dataansvarlige kan, hvis det findes nødvendigt og sagligt begrundet, anmode om at deltage i eller initiere en supplerende inspektion af en underdatabehandler. Databehandleren bistår så vidt muligt med kontakt og koordinering, dog inden for rammerne af den pågældende underdatabehandlers vilkår.
- Den dataansvarliges deltagelse i en inspektion hos en underdatabehandler ændrer ikke ved, at databehandleren fortsat har det fulde ansvar for underdatabehandlerens overholdelse af forordningen og disse Bestemmelser.

Bilag D Parternes regulering af andre forhold

Som supplement til Bestemmelse 11.1 kan den dataansvarlige, inden sletning gennemføres ved tjenestens ophør, anmode om at få udleveret eller eksporteret oplysningerne i det omfang og format, som tjenesten på ophørstidspunktet teknisk understøtter.