Databehandleraftale

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

mellem

Kunden

herefter "den dataansvarlige"

og

Lindhardt og Ringhof Forlag A/S
CVR-nr. 76351910
Vognmagergade 11
1120 København K
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

Indholdsfortegnelse

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 levering og drift af digitale læremidler via databehandlerens platform, jf. den til enhver tid gældende skriftlige aftale mellem den dataansvarlige og databehandleren, herunder de(n) ordrebekræftelse(r), vilkår og betingelser fremsendt af databehandleren samt tilkøb af digitale læremidler (herefter "Aftalen"), 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 præliminært 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 er omfattet af Bestemmelserne.

10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24),

databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[1] nationale ret og disse Bestemmelser.

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

4. Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.

2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

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 passende beskyttelsesniveau.

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

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 i sin aftale med underdatabehandleren, hvis muligt, 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 eller tilbagelevere 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.

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 dataansvarlig, 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 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 ved indgåelse af Aftalen og accept af Databehandlerens handelsbetingelser.

2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.

5. Underskrift

   Databehandleraftalen er accepteret af Kunden ved indgåelse af Aftalen og accept af Databehandlerens handelsbetingelser.

På vegne af databehandleren

Dato	
Navn	Kim Bjørn Tiedemann
Stilling	Direktør for teknologi og udvikling
Telefonnummer	+45 26 80 50 89
E-mail	Databehandling@lrforlag.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.

   Kontaktperson hos den dataansvarlige:

Navn:
Stilling:
Telefonnummer:
E-mail:

Kontakt hos den dataansvarlige ved sikkerhedsbrud jf. afsnit 10:
E-mail:

Kontaktperson hos databehandleren:

Navn:	Jonas Nielsen
Stilling:	Digital udviklingschef
Telefonnummer:	+45 6171 1712
E-mail:	Databehandling@lrforlag.dk

Bilag A Oplysninger om behandlingen

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

Formålet med behandlingen er at levere de tjenester, som den dataansvarlige har købt/licenseret af databehandleren.

Formålet med behandling af personoplysninger er at give adgang til databehandlerens digitale læremidler. De digitale læremidler udbydes i en portal på internettet, hvortil elever og lærere gives adgang. Forskellige undervisningsforløb kan herefter understøttes/gennemføres vha. en internetbrowser, en app eller andet formidlingsmedie.

Databehandleren behandler personoplysningerne for, at brugerne kan anvende databehandlerens digitale læremidler, herunder besvare opgaver, bedømme opgaver og foretage egen-evaluering af opgaveløsning, samt at brugerne kan få support, såfremt behovet skulle opstå.

Databehandleren behandler anonymiseret brugsdata til brug for rapportering til den dataansvarlige samt til statistiske formål, med henblik på at analysere brugen af de digitale læremidler og for løbende at sikre, at de digitale læremidler skaber optimalt læringsudbytte, er brugervenlige og lette at navigere i.

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

Databehandleren foretager følgende behandlinger af personoplysninger på vegne af den dataansvarlige:
Etablering af den dataansvarliges brugeres adgang til de digitale læremidler ved at elevers/læreres Unilogin-oplysninger overføres fra Styrelsen for It og Læring (STIL) til databehandleren i forbindelse med login.
Administration af brugernes adgange til tilknyttede læringsmoduler:
Opbevaring af de personoplysninger, som databehandleren modtager via STIL, og som brugerne potentielt indtaster ved brug af databehandlerens digitale læremidler
Behandling af anonymiserede forbrugsdata til brug for rapportering til den dataansvarlige, herunder den dataansvarliges institution(er), om anvendelsen af de digitale læremidler
Behandling af supporthenvendelser fra brugerne i forbindelse med anvendelsen af de digitale læremidler.

Ovennævnte aktiviteter indebærer at personoplysningerne bearbejdes som følger:

- indsamling,
- registrering,
- organisering,
- systematisering,
- opbevaring,
- tilpasning eller ændring,
- genfinding,
- søgning,

- brug,
- sletning/tilintetgørelse/anonymisering

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

A.3.1

REGISTRERETE / PERSON-OPLYSNINGER	Elever	Medarbejdere
Almindelige personoplysninger: (art. 6)	☐ Navn ☐ Adresse ☐ E-mail ☐ Telefonnummer ☐ Fødselsdato ☐ Medarbejder ID ☐ Billeder ☒ Andre almindelige personoplysninger: Der henvises til beskrivelse i A.3.2.	☐ Navn ☐ Adresse ☐ E-mail ☐ Telefonnummer ☐ Fødselsdato ☐ Medarbejder ID ☐ Billeder ☒ Andre almindelige personoplysninger: Der henvises til beskrivelse i A.3.2.
Følsomme personoplysninger: (art. 9)	☐ Race eller etnisk oprindelse ☐ Politisk, religiøs eller filosofisk overbevisning ☐ Fagforeningsmæssige tilhørsforhold ☐ Genetisk data ☐ Biometrisk data ☐ Helbredsoplysninger ☐ Seksuelle forhold eller orientering	☐ Race eller etnisk oprindelse ☐ Politisk, religiøs eller filosofisk overbevisning ☐ Fagforeningsmæssige tilhørsforhold ☐ Genetisk data ☐ Biometrisk data ☐ Helbredsoplysninger ☐ Seksuelle forhold eller orientering
Straffedomme og lovovertrædelser (§10)	☐ Straffedomme og lovovertrædelser	☐ Straffedomme og lovovertrædelser
CPR-nummer (§11)	☐ CPR-nummer	☐ CPR-nummer
Andre fortrolige personoplysninger	☐ Væsentlige sociale forhold ☐ Væsentlige økonomiske forhold ☐ Bankoplysninger ☐ Ansøgninger og CV ☐ Andre fortrolige oplysninger: [beskriv hvilke]	☐ Væsentlige sociale forhold ☐ Væsentlige økonomiske forhold ☐ Bankoplysninger ☐ Ansøgninger og CV ☐ Andre fortrolige oplysninger: [beskriv hvilke]

A.3.2. Andre almindelige personoplysninger
Behandlingen omfatter almindelige oplysninger, jf. databeskyttelsesforordningen. Behandlingen tager udgangspunkt i eksport af personoplysninger fra Uni-login (ws17/wsiEKSPORT, lille pakke) og omfatter fornavn(e) og efternavn.

Supplerende oplysninger om elever:

- Studietype (elev/studerende)
- Studienummer
- Elevens niveau (for grundskoleelever)

- Elevens hovedgruppe (klasse)
- Yderligere grupper elever er tilknyttet
- Afdeling, bygning eller værelsesnummer på efterskoler

Supplerende oplysninger om ansatte:

- Ansættelsestype (lærer, tap, pæd eller gæst)
- Initialer
- Stilling
- Afdeling, bygning eller værelsesnummer på efterskoler
- Grupper medarbejderen er tilknyttet

Oplysninger om UNI-login for ansatte og elever/studerende:

- Uni login-brugernavn (bruger-id)

Oplysninger om grupper på institutionen:

- Gruppe-id
- Gruppenavn
- Gruppetype
- Niveau
- Spor
- Startdato
- Slutdato

Ved brugen af de digitale læremidler behandles desuden følgende personoplysninger af databehandleren:

- Loginoplysninger,
- Pseudonymiseret bruger-id,
- IP-adresse,
- forbrugsdata,
- brugernes anvendelse af databehandlerens digitale læremidler (kliks, tidsforbrug mv.), herunder besvarelse af opgaver, bedømmelse af opgaver og egen-evaluering af opgaveløsning.

I forbindelse med levering af support behandles følgende:

- Navn
- E-mail (arbejdsmail)
- Telefonnummer (arbejdstelefon)
- Support tickets

A.4. Behandlingen omfatter følgende kategorier af registrerede

Der behandles oplysninger om følgende kategorier af registrerede:
A) Elever, herunder studerende.
B) Lærere, herunder pædagoger og andre, der har en undervisningsfunktion.
C) Administrativt personale, herunder personer med tilknytning til en uddannelsesinstitution.

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

Så længe databehandleren er i besiddelse af den dataansvarliges data.

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af parterne.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

VIRKSOMHEDENS NAVN OG ADRESSE SAMT CVR ELLER ANDET VIRKSOMHEDS ID	BESKRIVELSE AF BRUGEN AF UNDERDATABEHANDLERENS TJENESTER	LOKALITET FOR BEHANDLING SAMT EVENTUELT OVERFØRSELSGRUNDLAG
Sentia A/S	System: Digitale læremidler. Behandling: Hosting af digitale læremidler, herunder vedligehold af servere, backup, sikkerhed mv. Hosting sker i deres hostingcenter i Danmark.	EU
Microsoft Ireland Operations, Ltd. * One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland	System: Digitale læremidler. Behandling: Hosting af digitale læremidler, herunder vedligehold af servere, backup, sikkerhed mv.	EU/EØS.
Egmont Administration A/S (Egmont IT) Vognmagergade 11, 1148 København K CVR: 84853518	System: Digitale læremidler. Behandling: Drift af løsninger på Microsoft Azure og Amazon AWS, herunder administration af miljøer, overvågning, brugeradministration mv.	EU/EØS.
HubSpot One Dockland Central, Guild Street, Dublin 1, Co. Dublin, Ireland	System: Kundesupport på alle digitale læremidler. Behandling: Sagsstyringssystem til håndtering af kundehenvendelser. Tages i brug d. 4/10-2024	EU/EØS USA Overførselsgrundlag: EU Kommissionens tilstrækkelighedsafgørelse; DPF
Aircall	System: Telefonisystem	EU/EØS USA

VIRKSOMHEDENS NAVN OG ADRESSE SAMT CVR ELLER ANDET VIRKSOMHEDS ID	BESKRIVELSE AF BRUGEN AF UNDERDATABEHANDLERENS TJENESTER	LOKALITET FOR BEHANDLING SAMT EVENTUELT OVERFØRSELSGRUNDLAG
11 Rue Saint-Georges, 75009 Paris, France	Behandling: Håndtering af telefoni i forbindelse med kundehenvendelser. Der behandles telefonnummer på brugeren som ringer til support. Tages i brug d. 4/10-2024	Overførselsgrundlag: EU Kommissionens tilstrækkelighedsafgørelse; DPF

* Microsoft Ireland Operations er medtaget i ovenstående, da Lindhardt og Ringhof fører selvstændigt tilsyn med underdatabehandleren selvom aftalepartneren er Egmont IT.

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden at følge den aftalte procedure for udskiftning af underdatabehandlere – 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 indsigelse ved skift af underdatabehandlere

Den dataansvarlige kan gøre indsigelse mod tilføjelse af eller udskiftning af en underdatabehandler.

Den dataansvarliges eventuelle indsigelse skal meddeles ved skriftlig henvendelse til databehandleren. Modtager databehandleren ikke en skriftlig indsigelse inden 30 dage efter, at databehandleren har oplyst om en planlagt ændring af de angivne underdatabehandlere, anses ændringerne for godkendt af den dataansvarlige.

Modtager databehandleren en skriftlig indsigelse fra den dataansvarlige inden for 30 dage, og er indsigelsen konkret og sagligt begrundet, skal databehandleren tage indsigelsen til efterretning.

Hvis den dataansvarlige ikke kan acceptere en underdatabehandler, uden en konkret og saglig begrundelse bringes de(n) tjeneste(r), for hvilken underdatabehandleren deltager i behandlingsaktiviteter til ophør. Ophør af tjenesterne sker overensstemmelse med 14.4 i disse bestemmelser og de øvrige vilkår i Aftalen.

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:

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

Enhver behandling, som er nødvendig for, at databehandleren kan opfylde de forpligtelser, der er fastsat i Aftalen, herunder:

- Behandling af personoplysninger i forbindelse med brug af databehandlerens digitale læremidler, jf. Bilag A.
- Behandling af brugerhenvendelser via supportsystemer, jf. Bilag A og Bilag B.1.

Personoplysningerne behandles af databehandleren for at kunne stille indholdet på de digitale læremidler til rådighed for den enkelte bruger samt løbende at sikre, at de digitale læremidler er brugervenlige og lette at navigere i.

Databehandleren behandler desuden personoplysningerne for, at brugerne kan anvende databehandlerens digitale læremidler, herunder besvare opgaver, bedømme opgaver og foretage egen-evaluering af opgaveløsning, samt at brugerne kan få support, såfremt behovet skulle opstå.

Databehandleren behandler ligeledes personoplysninger for at kunne dokumentere overfor den dataansvarlige, hvor mange gange brugerne har logget sig på databehandlerens digitale læremidler (forbrugsdata).

Personoplysningerne kan endelig blive brugt i forbindelse med support af service og infrastruktur og databehandlerens logning.

C.2. Behandlingssikkerhed

C.2.1. Sikkerhedsniveauet skal afspejle behandlingens karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder. Som følge heraf har den dataansvarlige og databehandleren begge udarbejdet en risikoanalyse vedrørende databehandlingen og er enige om de foranstaltninger som er beskrevet i det følgende.

C.2.2. 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.

C.2.3. databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige herunder.

C.2.4. Databehandleren har vurderet, at de konkrete behandlingsaktiviteter medfører et lavt risikoniveau for de registrerede. Dog medfører det forhold, at behandlingen også vedrører almindelige persondata på børn, at databehandleren vælger at betragte risikoniveauet som “medium”. Databehandleren implementerer derfor et sikkerhedsniveau der modsvarer en risikovurdering på niveauet

”medium” jf. European Network and Information Security Agency’s (ENISA) “Handbook on Security of Personal Data Processing”.

ENISA’s bruttokatalog over anbefalede foranstaltninger til imødegåelse af et risikoniveau på ”LOW” (grøn) og ”MEDIUM” (gul) er angivet nedenfor:

	MEASURE CATEGORY	MEASURE IDENTIFIER	MEASURE DESCRIPTION
01-FORANSTALTNINGER VEDRØRENDE PSEUDONYMISERING OG KRYPTERING AF PERSONOPLYSNINGER			
	Server/Database security	**M.3**	Encryption solutions should be considered on specific files or records through software or hardware implementation.
	Server/Database security	**M.4**	Encrypting storage drives should be considered
	Server/Database security	**M.5**	Pseudonymization techniques should be applied through separation of data from direct identifiers to avoid linking to data subject without additional information
	Network/Communication security	**O.1**	Whenever access is performed through the Internet, communication should be encrypted through cryptographic protocols (TLS/SSL).
	Network/Communication security	**O.2**	Wireless access to the IT system should be allowed only for specific users and processes. It should be protected by encryption mechanisms.
02-FORANSTALTNINGER VEDRØRENDE EVNEN TIL AT SIKRE VEDVARENDE FORTROLIGHED, INTEGRITET, TILGÆNGELIGHED OG ROBUSTHED AF BEHANDLINGSSYSTEMER OG –TJENESTER			
	Security policy and procedures for the protection of personal data	**A.1**	The organization should document its policy with regards to personal data processing as part of its information security policy.
	Security policy and procedures for the protection of personal data	**A.2**	The security policy should be reviewed and revised, if necessary, on an annual basis.
	Security policy and procedures for the protection of personal data	**A.3**	The organization should document a separate dedicated security policy with regard to the processing of personal data. The policy should be approved by management and communicated to all employees and relevant external parties
	Security policy and procedures for the protection of personal data	**A.4**	The security policy should at least refer to: the roles and responsibilities of personnel, the baseline technical and organisation measures adopted for the security of personal data, the data processors or other third parties

			involved in the processing of personal data.
	Security policy and procedures for the protection of personal data	**A.5**	An inventory of specific policies/procedures related to the security of personal data should be created and maintained, based on the general security policy.
	Roles and responsibilities	**B.1**	Roles and responsibilities related to the processing of personal data should be clearly defined and allocated in accordance with the security policy.
	Roles and responsibilities	**B.2**	During internal re-organizations or terminations and change of employment, revocation of rights and responsibilities with respective hand over procedures should be clearly defined.
	Roles and responsibilities	**B.3**	Clear appointment of persons in charge of specific security tasks should be performed, including the appointment of a security officer.
	Access control policy	**C.1**	Specific access control rights should be allocated to each role (involved in the processing of personal data) following the need to know principle.
	Access control policy	**C.2**	An access control policy should be detailed and documented. The organization should determine in this document the appropriate access control rules, access rights and restrictions for specific user roles towards the processes and procedures related to personal data.
	Access control policy	**C.3**	Segregation of access control roles (e.g. access request, access authorization, access administration) should be clearly defined and documented.
	Resource/asset management	**D.1**	The organization should have a register of the IT resources used for the processing of personal data (hardware, software, and network). The register could include at least the following information: IT resource, type (e.g. server, workstation), location (physical or electronic). A specific person should be assigned the task of maintaining and updating the register (e.g. IT officer).
	Resource/asset management	**D.2**	IT resources should be reviewed and updated on regular basis.
	Resource/asset management	**D.3**	Roles having access to certain resources should be defined and documented.

	Change management	**E.1**	The organization should make sure that all changes to the IT system are registered and monitored by a specific person (e.g. IT or security officer). Regular monitoring of this process should take place.
	Change management	**E.2**	Software development should be performed in a special environment that is not connected to the IT system used for the processing of personal data. When testing is needed, dummy data should be used (not real data). In cases that this is not possible, specific procedures should be in place for the protection of personal data used in testing.
	Change management	**E.3**	A detailed and documented change policy should be in place. It should include: a process for introducing changes, the roles/users that have change rights, timelines for introducing changes. The change policy should be regularly updated.
	Data processors	**F.1**	Formal guidelines and procedures covering the processing of personal data by data processors (contractors/outsourcing) should be defined, documented and agreed between the data controller and the data processor prior to the commencement of the processing activities. These guidelines and procedures should mandatorily establish the same level of personal data security as mandated in the organization's security policy.
	Confidentiality of personnel	**I.1**	The organization should ensure that all employees understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities should be clearly communicated during the pre-employment and/or induction process.
	Confidentiality of personnel	**I.2**	Prior to up taking their duties employees should be asked to review and agree on the security policy of the organization and sign respective confidentiality and non-disclosure agreements.
	Training	**J.1**	The organization should ensure that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data should also be properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.
	Training	**J.2**	The organization should have structured and regular training programmes for staff, including specific programmers for the induction (to data protection matters) of newcomers.
	Access control and authentication	**K.1**	An access control system applicable to all users accessing the IT system should be implemented. The system should

			allow creating, approving, reviewing and deleting user accounts.
	Application lifecycle security	**R.1**	During the development lifecycle best practises, state of the art and well acknowledged secure development practices, frameworks or standards should be followed.
	Application lifecycle security	**R.2**	Specific security requirements should be defined during the early stages of the development lifecycle.
	Application lifecycle security	**R.3**	Specific technologies and techniques designed for supporting privacy and data protection (also referred to as Privacy Enhancing Technologies (PETs)) should be adopted in analogy to the security requirements.
	Application lifecycle security	**R.4**	Secure coding standards and practises should be followed.
	Application lifecycle security	**R.5**	During the development, testing and validation against the implementation of the initial security requirements should be performed.
	Application lifecycle security	**R.8**	Information about technical vulnerabilities of information systems being used should be obtained.
	Application lifecycle security	**R.9**	Software patches should be tested and evaluated before they are installed in an operational environment.
03-FORANSTALTNINGER VEDRØRENDE EVNEN TIL RETTIDIGT AT GENOPRETTE TILGÆNGELIGHEDEN AF OG ADGANGEN TIL PERSONOPLYSNINGER I TILFÆLDE AF EN FYSISK ELLER TEKNISK HÆNDELSE			
	Business continuity	**H.1**	The organization should establish the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing personal data (in the event of an incident/personal data breach).
	Business continuity	**H.2**	A BCP should be detailed and documented (following the general security policy). It should include clear actions and assignment of roles.
	Business continuity	**H.3**	A level of guaranteed service quality should be defined in the BCP for the core business processes that provide for personal data security.
	Back-ups	**P.1**	Backup and data restore procedures should be defined, documented and clearly linked to roles and responsibilities.
	Back-ups	**P.2**	Backups should be given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.

	Back-ups	**P.3**	Execution of backups should be monitored to ensure completeness.
	Back-ups	**P.4**	Full backups should be carried out regularly.
	Back-ups	**P.5**	Backup media should be regularly tested to ensure that they can be relied upon for emergency use.
	Back-ups	**P.6**	Scheduled incremental backups should be carried out at least on a daily basis.
	Back-ups	**P.7**	Copies of the backup should be securely stored in different locations.
	Back-ups	**P.8**	In case a third party service for back up storage is used, the copy must be encrypted before being transmitted from the data controller.
04-FORANSTALTNINGER VEDRØRENDE REGELMÆSSIG AFPRØVNING, VURDERING OG EVALUERING AF EFFEKTIVITETEN AF DE TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER TIL SIKRING AF BEHANDLINGSSIKKERHEDEN			
	Application lifecycle security	**R.6**	Vulnerability assessment, application and infrastructure penetration testing should be performed by a trusted third party prior to the operational adoption. The application shall not be adopted unless the required level of security is achieved.
	Application lifecycle security	**R.7**	Periodic penetration testing should be carried out.
05-FORANSTALTNINGER VEDRØRENDE ADGANG TIL OPLYSNINGERNE VIA INTERNETTET			
	Network/Communication security	**O.1**	Whenever access is performed through the Internet, communication should be encrypted through cryptographic protocols (TLS/SSL).
	Network/Communication security	**O.2**	Wireless access to the IT system should be allowed only for specific users and processes. It should be protected by encryption mechanisms.
	Network/Communication security	**O.3**	Remote access to the IT system should in general be avoided. In cases where this is absolutely necessary, it should be performed only under the control and monitoring of a specific person from the organization (e.g. IT administrator/security officer) through pre-defined devices.

	Network/Communication security	**O.4**	Traffic to and from the IT system should be monitored and controlled through Firewalls and Intrusion Detection Systems.
06-FORANSTALTNINGER VEDRØRENDE BESKYTTELSE AF OPLYSNINGER UNDER TRANSMISSION			
	Network/Communication security	**O.4**	Traffic to and from the IT system should be monitored and controlled through Firewalls and Intrusion Detection Systems.
07-FORANSTALTNINGER VEDRØRENDE BESKYTTELSE AF OPLYSNINGER UNDER OPBEVARING			
	Server/Database security	**M.1**	Database and applications servers should be configured to run using a separate account, with minimum OS privileges to function correctly.
	Server/Database security	**M.2**	Database and applications servers should only process the personal data that are actually neededs to process in order to achieve its processing purposes.
	Physical security	**T.1**	The physical perimeter of the IT system infrastructure should not be accessible by non-authorized personnel.
08-FORANSTALTNINGER VEDRØRENDE FYSISK SIKRING AF LOKALITETER, HVOR DER BEHANDLES OPLYSNINGER			
	Physical security	**T.2**	Clear identification, through appropriate means e.g. ID Badges, for all personnel and visitors accessing the premises of the organization should be established, as appropriate.
	Physical security	**T.3**	Secure zones should be defined and be protected by appropriate entry controls. A physical log book or electronic audit trail of all access should be securely maintained and monitored
	Physical security	**T.4**	Intruder detection systems should be installed in all security zones.
	Physical security	**T.5**	Physical barriers should, where applicable, be built to prevent unauthorized physical access.
	Physical security	**T.6**	Vacant secure areas should be physically locked and periodically reviewed
	Physical security	**T.7**	An automatic fire suppression system, closed control dedicated air conditioning system and uninterruptible power supply (UPS) should be implemented at the server room

	Physical security	**T.8**	External party support service personnel should be granted restricted access to secure areas.
09-FORANSTALTNINGER VEDRØRENDE ANVENDELSE AF HJEMME-/FJERNARBEJDSPLADSER			
	Workstation security	**N.1**	Users should not be able to deactivate or bypass security settings.
	Workstation security	**N.2**	Anti-virus applications and detection signatures should be configured on a weekly basis.
	Workstation security	**N.3**	Users should not have privileges to install or deactivate unauthorized software applications.
	Workstation security	**N.4**	The system should have session timeouts when the user has not been active for a certain time period.
	Workstation security	**N.5**	Critical security updates released by the operating system developer should be installed regularly.
	Workstation security	**N.6**	Anti-virus applications and detection signatures should be configured on a daily basis.
	Mobile/Portable devices	**Q.1**	Mobile and portable device management procedures should be defined and documented establishing clear rules for their proper use.
	Mobile/Portable devices	**Q.2**	Mobile devices that are allowed to access the information system should be pre-registered and pre-authorized.
	Mobile/Portable devices	**Q.3**	Mobile devices should be subject to the same levels of access control procedures (to the data processing system) as other terminal equipment.
	Mobile/Portable devices	**Q.4**	Specific roles and responsibilities regarding mobile and portable device management should be clearly defined.
	Mobile/Portable devices	**Q.5**	The organization should be able to remotely erase personal data (related to its processing operation) on a mobile device that has been compromised.
	Mobile/Portable devices	**Q.6**	Mobile devices should support separation of private and business use of the device through secure software containers.
	Mobile/Portable devices	**Q.7**	Mobile devices should be physically protected against theft when not in use.
10-FORANSTALTNINGER VEDRØRENDE LOGNING			

	Logging and monitoring	**L.1**	Log files should be activated for each system/application used for the processing of personal data. They should include all types of access to data (view, modification, deletion).
	Logging and monitoring	**L.2**	Log files should be timestamped and adequately protected against tampering and unauthorized access. Clocks should be synchronised to a single reference time source
	Logging and monitoring	**L.3**	Actions of the system administrators and system operators, including addition/deletion/change of user rights should be logged.
	Logging and monitoring	**L.4**	There should be no possibility of deletion or modification of log files content. Access to the log files should also be logged in addition to monitoring for detecting unusual activity.
	Logging and monitoring	**L.5**	A monitoring system should process the log files and produce reports on the status of the system and notify for potential alerts.
11-FORANSTALTNINGER UDENFOR DATATILSYNETS KATEGORISERING			
	Data processors	**F.2**	Upon finding out of a personal data breach, the data processor shall notify the controller without undue delay.
	Data processors	**F.3**	Formal requirements and obligations should be formally agreed between the data controller and the data processor. The data processor should provide sufficient documented evidence of compliance.
	Data processors	**F.4**	The data controller's organization should regularly audit the compliance of the data processor to the agreed level of requirements and obligations.
	Incidents handling / Personal data breaches	**G.1**	An incident response plan with detailed procedures should be defined to ensure effective and orderly response to incidents pertaining personal data.
	Incidents handling / Personal data breaches	**G.2**	Personal data breaches should be reported immediately to the management. Notification procedures for the reporting of the breaches to competent authorities and data subjects should be in place, following art. 33 and 34 GDPR.
	Incidents handling / Personal data breaches	**G.3**	The incidents' response plan should be documented, including a list of possible mitigation actions and clear assignment of roles.

	Access control and authentication	**K.2**	The use of common user accounts should be avoided. In cases where this is necessary, it should be ensured that all users of the common account have the same roles and responsibilities.
	Access control and authentication	**K.3**	An authentication mechanism should be in place, allowing access to the IT system (based on the access control policy and system). As a minimum a username/password combination should be used. Passwords should respect a certain (configurable) level of complexity.
	Access control and authentication	**K.4**	The access control system should have the ability to detect and not allow the usage of passwords that don't respect a certain (configurable) level of complexity.
	Access control and authentication	**K.5**	A specific password policy should be defined and documented. The policy should include at least password length, complexity, validity period, as well as number of acceptable unsuccessful login attempts.
	Access control and authentication	**K.6**	User passwords must be stored in a "hashed" form.
	Data deletion/disposal	**S.1**	Software-based overwriting should be performed on all media prior to their disposal. In cases where this is not possible (CD's, DVD's, etc.) physical destruction should be performed.
	Data deletion/disposal	**S.2**	Shredding of paper and portable media used to store personal data shall be carried out.
	Data deletion/disposal	**S.3**	Multiple passes of software-based overwriting should be performed on all media before being disposed.
	Data deletion/disposal	**S.4**	If a third party's services are used to securely dispose of media or paper based records, a service agreement should be in place and a record of destruction of records should be produced as appropriate.

Databehandleren afvender som nævnt en kategorisering af foranstaltninger som er anbefalet af ENISA1 i databehandlerens styring af Governance, Risk management og Compliance (GRC) aktiviteterne. Ovenfor er ENISA's anbefalede foranstaltninger til risikoniveau "LOW" og "MEDIUM", mappet til kategorisering af foranstaltninger, jf. bilag C.2 i Datatilsynets skabelon til databehandleraftale.
En given ENISA foranstaltning kan være gentaget, da den kan være relevant for flere af Datatilsynets kategorier og der er også foranstaltninger, som ikke kan mappes til Datatilsynets kategorier.

Datatilsynets kategori "04-FORANSTALTNINGER VEDRØRENDE REGELMÆSSIG AFPRØVNING, VURDERING OG EVALUERING AF EFFEKTIVITETEN AF DE TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER TIL SIKRING AF BEHANDLINGSSIKKERHEDEN" er ikke direkte henførbar til en tilsvarende foranstaltningskategori i ENISA's katalog, men databehandleren foretager regelmæssig evaluering af foranstaltninger, dels i forbindelse med gennemførelse af opgaver i databehandlerens årshjul, dels i forbindelse med den årlige udarbejdelse af ISAE3000 revisionserklæring.

Databehandleren har implementeret de ovenfor nævnte foranstaltninger, med enkelte undtagelser for specifikke ældre produkter. Databehandleren har redegjort for undtagelserne

her: https://www.alinea.dk/lr-sikkerhedsforanstaltninger

Databehandlerens sikkerhedsforanstaltninger er ikke begrænset til det, der er fastsat i ovenstående beskrivelse og skal om nødvendigt, tilpasses løbende med henblik på at sikre et passende sikkerhedsniveau i forhold til risikoen.
Databehandleren orienterer den dataansvarlige hvis sikkerhedsforanstaltninger ændres væsentligt.

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 vederlægges for bistand til den dataansvarlige i overensstemmelse med Hovedaftalen.

Underretning af den dataansvarlige om anmodninger fra de registrerede
Databehandleren skal uden unødig forsinkelse, efter at være blevet opmærksom herpå, skriftligt underrette den dataansvarlige om enhver anmodning rettet til databehandleren eller dennes underdatabehandlere fra en registreret om udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret. Databehandleren er ikke berettiget til at besvare anmodninger fra en registreret vedrørende udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret. Databehandleren skal på anmodning fra den dataansvarlige hjælpe med at opfylde den dataansvarliges forpligtelser i forhold til de registreredes rettigheder i henhold til gældende databeskyttelsesret.

Bistand ved sikkerhedsbrud, herunder underretning af den dataansvarlige om sikkerhedsbrud
Databehandlerens bistand i forbindelse med den dataansvarliges forpligtelser efter databeskyttelsesforordningens artikel 33 og 34 sker ved, at databehandleren indgiver de oplysninger, der følger af Bestemmelse 10.3, til den dataansvarlige inden for den frist, der følger af Bestemmelse 10.2. Databehandleren skal efterfølgende bistå den dataansvarlige ved på den dataansvarliges anmodning at stille de oplysninger til rådighed, som er nødvendige for, at den dataansvarlige kan foretage anmeldelse af brud på persondatasikkerheden til den kompetente tilsynsmyndighed eller som er nødvendige for, at den dataansvarlige kan underrette den registrerede herom.

Bistand i forbindelse med risikovurderinger og konsekvensanalyser
Databehandleren skal bistå den dataansvarlige ved at stille de nødvendige oplysninger til rådighed, så den dataansvarlige kan gennemføre de nødvendige risikovurderinger. Såfremt den dataansvarlige vurderer, at behandlingen sandsynligvis vil indebære en høj risiko for de registreredes rettigheder og frihedsrettigheder, skal databehandleren på anmodning fra den dataansvarlige bistå den dataansvarlige i forbindelse med dennes forpligtelser efter databeskyttelsesforordningens artikel 35 og 36 ved at indgive de oplysninger til den dataansvarlige, der er nødvendige for, at den dataansvarlige kan foretage en konsekvensanalyse i overensstemmelse med artikel 35 og foretage en forudgående høring af den kompetente tilsynsmyndighed i overensstemmelse med artikel 36.

Sikring af tekniske og organisatoriske foranstaltninger
Databehandleren skal endelig sikre, at dennes tekniske og organisatoriske foranstaltninger gør det muligt for den dataansvarlige at overholde sine forpligtelser efter databeskyttelsesforordningens artikel 33-36, herunder f.eks. gennem de foranstaltninger vedrørende styring af sikkerhedsbrud, styring af aktiver, logning mv., der følger af bilag C.

C.4 Opbevaringsperiode/sletterutine

Personoplysningerne opbevares hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret.

Ved ophør af tjenesten eller disse Bestemmelser vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarliges oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

Der kan læses mere om databehandlerens løbende sletning og retention perioder på Alineas side om sikkerhedsforanstaltninger: https://www.alinea.dk/lr-sikkerhedsforanstaltninger

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:

Virksomhedens navn og adresse	CVR eller andet virksomheds ID	Lokalitet for behandling	Eventuelt overførselsgrundlag
Sentia A/S Lyskær 3A, DK-2730 Herlev, Danmark	CVR: 10008123	EU/EØS.	N/A
Microsoft Ireland Operations, Ltd. One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland		EU/EØS.	N/A
Egmont Administration A/S (Egmont IT) Vognmagergade 11, 1148 København K CVR: 84853518	CVR: 84853518	EU/EØS.	N/A
HubSpot One Dockland Central, Guild Street, Dublin 1, Co. Dublin, Ireland		EU/EØS USA	Overførselsgrundlag: EU Kommissionens tilstrækkelighedsafgørelse; DPF
Aircall 11 Rue Saint-Georges, 75009 Paris, France		EU/EØS USA	Overførselsgrundlag: EU Kommissionens tilstrækkelighedsafgørelse; DPF

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.

Den dataansvarlige giver ved indgåelsen af denne aftale skriftlig instruks til databehandleren i at overføre personoplysninger til tredjelande i forbindelsen med tilføjelser af underdatabehandlere i det omfang, dette er nødvendigt for leveringen af tjenesterne.

Ved overførsel af personoplysninger til tredjelande er databehandleren ansvarlig for, at der foreligger et gyldigt overførselsgrundlag.

Gyldigt overførselsgrundlag for overførslerne er navnlig:

1. En afgørelse om tilstrækkeligheden af beskyttelsesniveauet i henholdt databeskyttelsesforordningens artikel 45 eller
2. EU-Kommissionens standardkontraktbestemmelser i henhold til databeskyttelsesforordningens artikel 46, når databehandleren samtidig vurderer – og i nødvendigt omfang implementerer supplerende foranstaltninger med henblik på at sikre – den pågældende overførelses lovlighed

Databehandleren skal underrette den Dataansvarlige om enhver henvendelse, som Databehandleren eller dennes underdatabehandlere modtager fra en myndighed i et tredjeland om videregivelse af personoplysninger omfattet af disse Bestemmelser.

Såfremt Databehandleren, direkte eller indirekte, modtager en anmodning om at udlevere oplysninger omfattet af disse Bestemmelser, herunder personoplysninger, til en modtager, der geografisk er placeret uden for EU/EØS, er Databehandleren til enhver tid forpligtet til at modsætte sig en sådan anmodning om udlevering, så vidt det er muligt for Databehandleren i henhold til EU-ret eller medlemsstaternes nationale ret.

Databehandleren skal, eventuelt i fællesskab med den pågældende underdatabehandler, udtømme enhver mulighed for at påklage anmodninger om videregivelse af personoplysninger omfattet af disse Bestemmelser, hvis der er tale om generelle anmodninger eller anmodninger, der ikke er i overensstemmelse med EU-retten, herunder databeskyttelsesforordningen, samt øvrig national lovgivning, som supplerer databeskyttelsesforordningen. Databehandleren skal, i det omfang det er muligt, give den Dataansvarlige mulighed for at indtræde i klage- og retssager, med henblik på at give den Dataansvarlige mulighed for at varetage sine egne interesser.

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

Databehandleren vil én gang årligt enten fremsende eller på sin hjemmeside fremlægge en erklæring om overholdelse af denne aftale. Erklæringen skal udarbejdes i overensstemmelse med gældende, anerkendte branchestandarder. Databehandleren tilstræber i april måned at offentliggøre erklæring for den senest afsluttede erklæringsperiode.

Den dataansvarlige kan gennemføre revision, inspektion eller tilsyn hos databehandleren, når den dataansvarlige finder det nødvendigt og i det omfang, at det ønskede emne for inspektionen eller tilsynet ikke allerede er adresseret i erklæringen nævnt ovenfor.

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

Databehandleren fører tilsyn med underdatabehandlere. Databehandleren fører tilsyn med underdatabehandlere i form af vurderinger af revisionserklæringer, fysiske besigtigelser eller skrivebordstilsyn. Valget af tilsynsform er baseret på karakteren af underdatabehandleren og den overladte behandling af personoplysninger.

Bilag D Parternes regulering af andre forhold

D.1 Databehandlerkæden

Databehandleren skal identificere – og kortlægge – underdatabehandlere, som behandler personoplysninger på vegne af databehandleren samt disses underdatabehandlere. Denne kortlægning skal ikke omfatte underdatabehandlere, som databehandleren – ud fra tekniske, organisatoriske og kontraktuelle foranstaltninger – kan sandsynliggøre ikke behandler den dataansvarliges personoplysninger.