

DATABEHANDLERAFTALE

KALTURA (herefter Systemet)

Standardkontraktbestemmelser

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

DeiC

CVR 30 06 09 46

Asmussens Allé

Bygning 305

2800 Lyngby

Denmark

herefter "databehandleren"

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

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

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

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 Systemet 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 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 medlemsstaternes¹ nationale ret og disse Bestemmelser.

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

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.
3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

4. Databehandleren handler efter instruks

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

5. Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.
2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

- a. Pseudonymisering og kryptering af personoplysninger

- b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
 - c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
 - d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.
2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.
 3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

4. Parternes eventuelle regulering/aftale om vederlæggelse eller lign. i forbindelse med den dataansvarliges eller databehandlerens efterfølgende krav om etablering af yderligere sikkerhedsforanstaltninger vil fremgå af denne aftales bilag D.

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 indføre 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 standardkontraktbestemmelser 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. indsigt retten
 - 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 unødigt 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 unødigt forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis

vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

Side 8 af 18

- 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 unødigt 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.

Side 9 af 18

2. Følgende regler i EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne efter ophør af tjenesterne vedrørende behandling af personoplysninger:
 - a. Data der er nødvendige at bevare i forhold til bogføring og regnskabsmæssige formål

Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

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

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

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

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

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

- At dataansvarliges brugere kan uploade videoer, og andre medier til Systemet, til visning og deling via portaler som LMS, CMS mm. For at sikre korrekt deling af medier får de dataansvarliges brugere adgang til hinandens navne, emailadresser og brugernavne under Systemet.

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

- At underdatabehandleren stiller Systemet til rådighed for databehandleren og den dataansvarlige og herigennem opbevarer personoplysninger om den dataansvarliges medlemmer på underdatabehandlerens servere.

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

- Navn
- E-mailadresse
- Brugernavn
- Organisation
- Gruppetilhørsforhold
- Lyd og videooptagelser

De fem 5 første typer af personoplysninger defineres som almindelige persondata jf. persondataforordningen.

Lyd og videooptagelse kan indeholde både almindelige og følsomme persondata. Derudover kan data være fortrolige.

A.4. Behandlingen omfatter følgende kategorier af registrerede

- Ansatte
- Studerende
- Øvrige brugere
- Personer som figurerer eller omtales i de lyd- og videofiler, der oplagres i tjenesten

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

- Behandlingen er ikke tidsbegrænset og varer indtil aftalen opsiges eller ophæves af en af parterne.

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
NORDUnet	17490346	Kastruplundgade 22, DK2770	Drift af servere, hvorpå ovenstående nævnte personoplysninger og data lagres, installationer og datasikkerhedsforanstaltninger. Fysisk sker dette på datacentre i Ørestaden og Ballerup.
Kaltura Europe Ltd	GB135656893	Northumberland House 4th Floor 303-306 High Holborn London WC1V 7JZ Great Britain	Support- og driftsopgaver
AmberScript B.V.	70427585	Keizersgracht 668B, 1017ET Amsterdam The Netherlands	Bruger af AWS-center i Frankfurt, Tyskland, hvor databehandling af mediefiler finder sted mht. transskription. Gælder alene brugere af REACH-modulet under Kaltura.

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet.

B.2. Varsel for godkendelse af underdatabehandlere

Side 13 af 18

Databehandleren må alene gøre brug af andre underdatabehandlere efter generel skriftlig godkendelse fra databehandleren på vegne af den dataansvarlige. Databehandlerens anmodning herom skal være databehandleren i hænde minimum 30 dage før anvendelsen eller ændringen skal træde i kraft. Afvisning af godkendelse skal ske senest 2 uger fra modtagelse af anmodning.

C.1. Behandlingens genstand/instruks

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

- Drift af servere og tilhørende datalagringsinfrastruktur, herunder datasikkerhedsforanstaltninger, hvorved ovenstående nævnte personoplysninger og data lagres.
- Den dataansvarlige er indforstået med, at systemet kan bruges af den dataansvarliges brugere til at offentliggøre indhold, som derfor ikke er omfattet af alle ovenstående foranstaltninger.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

- At der er tale om behandling af video- og audiomateriale med identificerbare personer. Audio- og videomaterialet kan indeholde personoplysninger. Vedhæftede dokumenter kan indeholde alle former for personoplysninger.

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:

C.2.1 Tekniske foranstaltninger til sikring af vedvarende fortrolighed, tilgængelighed, integritet**Fysisk adgangskontrol og sikring af udstyr**

Omfatter både indendørs og udendørs sikring, fx i form af elektronisk adgangskontrol og overvågning, adgangskontrol på hardware, serverrum og mekanisk sikring af terminaler og servere mod tyveri. Lokalteterne er sikret med fysiske foranstaltninger mht. ildebrand og strømudfald.

Brug af stærke adgangskoder – hvor WAYF ikke benyttes

Skal mindst indeholde 8 karakterer

Skal mindst indeholde 1 lille bogstav og 1 stort bogstav

Skal mindst indeholde 1 tal eller specialtegn (fx !, \$, #, %)

To-faktor-autentifikation

To-faktor-autentifikation er et ekstra lag af sikkerhedsniveau til fx en konto. For at kunne logge ind på sin konto skal brugeren foruden sin adgangskode også anvende et andet trin til bekræftelsen af sin identitet. Systemet rummer faciliteter til dette, som en administrator hos den dataansvarlige kan aktivere.

Adgang til data

Adgang til data sker via standard-understøttelser i Systemet, herunder Systemets generiske login-metode, LDAP og SAML.

Databehandlerens adgang til data sker via PoLP (Principle of Least Privilege)

Så få administratorer som muligt har adgang til servere og indhold, og afstemt efter behov.

Kryptering

Data beskyttes med kryptering i transmissionen og opbevares i et krypteret filsystem. Set fra Systemet kan data derimod tilgås uden kryptering, da det er en del af funktionaliteten i Systemet.

Logning

Logning sker ud fra standardindstillinger i Systemet, hvorudfra databehandler og den dataansvarlige har adgang til forbrugsstatistik.

Spejling af diske

Data beskyttes via spejling af diske (RAID 50), samt via dublering af indhold til 2 lokaliteter.

Backup

Backup af kundedata er ikke en del af aftalen. Derimod laves der backup af brugerdata konfiguration osv., som opbevares på et krypteret disksystem.

Opdatering af klienter og servere

Systemsoftware er sikret via løbende opdateringer.

Firewall

Systemet er sikret med firewall.

Netværkssegmentering

Netværkssegmentering er anvendt for Systemet, der er adskilt fra andre services i driftsceneteret.

Intrusion detection and prevention systems (IDPS)

Systemets produktions-firewall benytter IDPS, som bidrager til et lag af sikkerhed.

Reparation, service og skrotning

Reparation og service af dataudstyr foregår internt i huset af egne IT-medarbejdere. Skrotning af IT-udstyr sker via fast samarbejdspartner, som sikrer korrekt datasletning

C.2.2 Organisatoriske foranstaltninger til sikring af vedvarende fortrolighed, tilgængelighed, integritet

Databehandleren og dennes underdatabehandlere benytter kvalitetsstyring på sikkerhedsområdet, som bl.a. betyder at man har:

- Organisatorisk forankret IT-sikkerhedspolitik
- Information security management system (ISMS)
- Identity access governance (fx personalesikkerhedsprocedure)
- Change management
- Løbende identifikation og sikring af regler og praksis

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:

- Driftsmeddelelser udsendes via "serviceinfo.dk"

- Ved brud vil der ske henvendelse til den/de berørte institutioner via mail eller telefon
- Der tilbydes supplerende træning og uddannelse gennem webinar og workshops
- Anden support og teknisk bistand efter aftale med den tjenesteansvarlige

C.4 Opbevaringsperiode/sletterutine

Personoplysninger og data opbevares hos underdatabehandleren, indtil den dataansvarlige og dennes brugere selv sletter materialet, eller indtil databehandleren, på vegne af den dataansvarlige, anmoder om at få oplysninger og materiale slettet.

C.5 Lokaltet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

- To datacentre på to forskellige lokaliteter i Storkøbenhavn.

Underdatabehandleren kan kun overføre personoplysninger til et andet land i Norden efter skriftlig godkendelse af databehandleren, på vegne af den dataansvarlige.

Den dataansvarlige kan alene nægte godkendelse, såfremt den dataansvarlige har rimelige, konkrete årsager hertil. Afvisning af godkendelse skal ske senest 3 uger fra modtagelse af anmodning.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelände

Databehandleren kan kun overføre personoplysninger til anden tredjelände efter skriftlig godkendelse af den dataansvarlige.

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

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

Databehandleren udarbejder årligt et internt tilsyn, som stilles til rådighed for den dataansvarlige. Den dataansvarlige kan i løbet af året stille spørgsmål til databehandleren. Disse spørgsmål kan tages op af tilsynet, hvis det vurderes at være relevant.

Den dataansvarlige, eller en repræsentant for den dataansvarlige, kan efterspørge yderligere dokumentation, eller foretage et fysisk tilsyn vedrørende overholdelsen af denne databehandleraftale hos databehandleren. Den dataansvarlige skal dog betale de udgifter, databehandleren i den forbindelse bliver påført.

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

Den dataansvarlige kan – hvis det findes nødvendigt – vælge at initiere og deltage på en fysisk inspektion hos underdatabehandleren. Dette kan blive aktuelt, såfremt den dataansvarlige vur-

derer, at databehandlerens tilsyn med underdatabehandleren ikke har givet den dataansvarlige tilstrækkelig sikkerhed for, at behandlingen hos underdatabehandleren sker i overensstemmelse med denne databehandleraftale.

Den dataansvarliges eventuelle deltagelse i et tilsyn hos underdatabehandleren ændrer ikke ved, at databehandlerens ansvar for underdatabehandlerens overholdelse af databeskyttelseslovgivningen og denne databehandleraftale.

Databehandlerens og underdatabehandlerens eventuelle udgifter i forbindelse med afholdelse af et fysisk tilsyn/en inspektion hos underdatabehandleren skal afholdes af den dataansvarlige, hvis det er denne, der har foranlediget tilsynet.

D.1. Databehandlers vederlag og kompensation i forbindelse med særlige ydelser

I forbindelse med enhver tilsynsaktivitet, som ligger ud over C.7, vil databehandler gøre krav på fakturering af udgifter, herunder også internt arbejdsforbrug på timebasis svarende til DKK 900 per time.

D.2. Parternes ansvar ved ulovlig instruks

I det tilfælde at den dataansvarlige har givet en instruks, der senere viser sig at være i modstrid med gældende ret, vil den dataansvarlige være ene- ansvarlig for instruksens. Medmindre at databehandleren ikke ophører med at udføre instruksens efter denne er blevet informeret om, at instruksens er ulovlig.