DATABEHANDLERAFTALE

MELLEM

CLIO ONLINE APS OG UNDERVISNINGSINSTITUTIONER

DATABEHANDLERAFTALE

Mellem

Institutionens navn

Institutions nr.

Kommune

Adresse

CVR. nr.

(herefter "Institutionen")

og

Clio Online ApS
Esplanaden 8A, 1-2 sal
1263 København K
CVR. nr.: 30583795
herefter "Leverandøren"

er der indgået nedenstående databehandleraftale (herefter "Aftalen") om Leverandørens behandling af personoplysninger på vegne af Institutionen:

1. Aftalens baggrund, formål og udformning

1.1 Som producent og leverandør af digitale læremidler behandler Leverandøren personoplysninger med særligt henblik på at styrke elevprogression og feedback i forbindelse med både lærerfeedback og selvevaluering hos den enkelte elev. Leverandørens behandlinger og formålet med behandlingerne er beskrevet i Leverandørens Købsaftale og abonnementsbetingelserne heri.

1.2 Aftalen er udformet på baggrund af de anbefalinger, som Kommunernes Landsforening har givet landets kommuner i forhold til at sikre, at disse lever op til forpligtelserne til at efterleve den nye Databeskyttelsesforordning, som finder anvendelse fra 25. maj 2018.

1.3 Aftalen skal ses som et led i, at Leverandøren ønsker at understøtte vores kunder (kommuner, folkeskoler samt privat- og efterskoler på bedst muligvis vis i deres arbejde med at kunne leve op til Databeskyttelsesforordningen.

2. Om Clio Online ApS

Clio Online ApS er den største producent af digitale læremidler til den danske grundskole. I forbindelse med at udvikle og levere digitale læremidler og andre digitale løsninger til landets skoler behandler Clio Online ApS en række personoplysninger om både lærere og elever. Behandlingen sker ligeledes med henblik på at skabe den mest optimale brug af produkterne.

3. Generelt

3.1 Aftalen vedrører Leverandørens forpligtelse til at efterleve de sikkerhedskrav, som fremgår af Lov nr. 429 af 31/05/2000 med senere ændringer om behandling af personoplysninger (Persondataloven) § 42, jf. § 41, stk. 3-5. Kravene er beskrevet i:

(i) Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsbekendtgørelsen).

(ii) Vejledning nr. 37 af 02/04/2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsvejledningen).

3.2 Den 25. maj 2018 erstattes Persondataloven af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 (herefter Databeskyttelsesforordningen) således, at Aftalens pkt. 1.1 (i) – (ii) herefter erstattes med Databeskyttelsesforordningen.

3.3 I Aftalen er indarbejdet de krav, som såvel Persondataloven som de kommende regler i Databeskyttelsesforordningen stiller til databehandleraftaler.

3.4 Leverandøren skal behandle personoplysninger i overensstemmelse med god databehandlingsskik, jf. de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

4. Institutionens rettigheder og forpligtelser

4.1 Institutionen er dataansvarlig for de personoplysninger, som Institutionen instruerer Leverandøren om at behandle. Institutionen har ansvaret for, at de personoplysninger, som Institutionen instruerer Leverandøren om at behandle, må behandles af Leverandøren, herunder at behandlingen er nødvendig og saglig i forhold til Institutionens opgavevaretagelse.

4.2 Institutionen har de rettigheder og forpligtelser, som er givet en dataansvarlig i medfør af lovgivningen, jf. Aftalens pkt. 3.1 og 3.2.

5. Leverandørens forpligtelser

5.1 Leverandøren er databehandler for de personoplysninger, som Leverandøren behandler på vegne af Institutionen, jf. pkt. 6 og bilag 3. Leverandøren har som databehandler de forpligtelser, som er pålagt en databehandler i medfør af lovgivningen, jf. Aftalens pkt. 3.1 og 3.2.

5.2 Leverandøren behandler alene de overladte personoplysninger efter instruks fra Institutionen, jf. pkt. 6 og bilag 3, og alene med henblik på opfyldelse af "Købsaftalen" samt at skabe den bedste brugeroplevelse.

5.3 Leverandøren skal fra 25. maj 2018 løbende føre en fortegnelse over behandlingen af personoplysninger samt en fortegnelse over alle sikkerhedsbrud.

5.4 Leverandøren skal sikre personoplysningerne via tekniske og organisatoriske sikkerhedsforanstaltninger, som beskrevet i Sikkerhedsbekendtgørelsen og Sikkerhedsvejledningen (frem til 25. maj 2018) og Databeskyttelsesforordningen (fra 25. maj 2018), jf. bilag 1 – Sikkerhed.

5.5 Leverandøren skal på opfordring fra Institutionen hjælpe med at opfylde Institutionens forpligtelser i forhold til den registreredes rettigheder, herunder besvarelse af anmodninger fra borgere om indsigt i egne oplysninger, udlevering af borgerens oplysninger, rettelse og sletning af oplysninger, begrænsning af behandling af borgerens oplysninger, samt Institutionens forpligtelser i forhold til underretning af den registrerede ved sikkerhedsbrud, fra 25. maj 2018 i medfør af Databeskyttelsesforordningens kap. III samt artikel 34.

5.6 Leverandøren skal fra 25. maj 2018 hjælpe Institutionen med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens artikel 32-36.

5.7 Leverandøren garanterer fra 25. maj 2018 at levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger sådan, at Leverandørens behandling af Institutionens personoplysninger opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

5.8 Leverandøren er forpligtet til at oplyse med præcise adresseangivelser, hvor Institutionens personoplysninger opbevares, jf. bilag 2. Leverandøren skal ajourføre oplysningerne over for Institutionen ved enhver ændring.

5.9 Hvis Leverandøren er etableret i en anden EU-medlemsstat, skal Leverandøren frem til 25. maj 2018 ligeledes overholde de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat.

6. Underleverandør (underdatabehandler)

6.1 Ved underdatabehandler forstås en underleverandør, til hvem Leverandøren har overladt hele eller dele af den behandling, som Leverandøren foretager på vegne af Institutionen.

6.2 Leverandøren har ret til at anvende andre databehandlere end dem, som er angivet i bilag 2, til at behandle de personoplysninger, som Institutionen har overladt til Leverandøren i medfør af "Købsaftalen". Leverandøren skal ajourføre oplysninger om underdatabehandlere i bilag 2 ved enhver ændring. Institutionen kan ikke nægte at godkende tilføjelse eller udskiftning af en underdatabehandler, medmindre der foreligger en konkret saglig begrundelse herfor.

6.3 Hvis Leverandøren overlader behandlingen af personoplysninger, som Institutionen er dataansvarlig for, til underdatabehandlere, skal Leverandøren indgå en skriftlig (under)databehandleraftale med underdatabehandleren.

6.4 Underdatabehandleraftalen, jf. pkt. 6.3, skal pålægge underdatabehandleren de samme databeskyttelsesforpligtelser, som Leverandøren er pålagt efter Aftalen, herunder, at underdatabehandleren fra 25. maj 2018 garanterer at kunne levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at kunne implementere de passende tekniske og organisatoriske foranstaltninger således, at underdatabehandlerens behandling opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

6.5 Når Leverandøren overlader behandlingen af personoplysninger, som Institutionen er dataansvarlig for, til underdatabehandlere, har Leverandøren over for Institutionen ansvaret for underdatabehandlernes overholdelse af disses forpligtelser, jf. pkt. 6.3.

6.6 Institutionen kan til enhver tid forlange dokumentation fra Leverandøren for eksistensen og indholdet af underdatabehandleraftaler for de underdatabehandlere, som Leverandøren anvender i forbindelse med opfyldelsen af sine forpligtelser over for Institutionen.

6.7 Al kommunikation mellem Institutionen og underdatabehandleren sker via Leverandøren.

7. Instrukser

7.1 Leverandørens behandling af personoplysninger på vegne af Institutionen sker udelukkende efter dokumenteret instruks, jf. bilag 3. Det er leverandørens ansvar at sikre, at eventuelle underdatabehandlere jf. pkt. 6.3., får tilsendt Institutionens instruks, jf. bilag 3.

7.2 Leverandøren giver fra 25. maj 2018 omgående besked til Institutionen, hvis en instruks efter Leverandørens vurdering er i strid med lovgivningen, jf. pkt. 3.2.

8. Tekniske og organisatoriske sikkerhedsforanstaltninger

8.1 Leverandøren skal frem til 25. maj 2018, jf. bilag 1, træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger:

(i) tilintetgøres, mistes, ændres eller forringes,
(ii) kommer til uvedkommendes kendskab eller misbruges, eller

(iii) i øvrigt behandles i strid med lovgivningen, jf. pkt. 3.1

8.2 Leverandøren skal fra 25. maj 2018, jf. bilag 1, iværksætte alle sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.

8.3 Leverandøren skal [mindst en gang årligt] gennemgå sine interne sikkerhedsforskrifter og retningslinjer for behandlingen af personoplysninger med henblik på at sikre, at de fornødne sikkerhedsforanstaltninger til stadighed er iagttaget, jf. pkt. 8.1 og 8.2, samt bilag 1.

8.4 Leverandøren samt dennes ansatte er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.

8.5 Leverandøren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af Institutionens personoplysninger, om Leverandørens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed, jf. pkt 10.

8.6 Leverandøren er forpligtet til straks at underrette Institutionen om ethvert sikkerhedsbrud uanset, om dette sker hos Leverandøren eller hos en underdatabehandler.

9. Overførsler til andre lande

9.1 Leverandørens overførsel af personoplysninger til lande, der ikke er medlem af EU (tredjelande), f.eks. via en cloudløsning eller en underdatabehandler, skal ske i overensstemmelse med Institutionens instruks herfor, jf. bilag 3.

9.2 Ved overførsel til tredjelande er Leverandøren og Institutionen i fællesskab ansvarlige for, at der foreligger et gyldigt overførselsgrundlag.

9.3 Hvis Institutionens personoplysninger overføres til en EU-medlemsstat, er det frem til 25. maj 2018 Leverandørens ansvar, at de til enhver tid gældende bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat, overholdes.

10. Tavshedspligt og fortrolighed

10.1 Leverandøren er - under og efter Aftalens ophør - pålagt fuld tavshedspligt omkring alle oplysninger, denne bliver bekendt med gennem samarbejdet. Aftalen indebærer, at tavshedspligtsbestemmelserne i straffelovens §§ 152-152f, jf. straffelovens § 152a, finder anvendelse.

10.2 Leverandøren skal fra 25. maj 2018 sikre, at alle, der behandler oplysninger omfattet af "Købsaftalen", herunder ansatte, tredjeparter (f.eks. en reparatør) og underdatabehandlere, forpligter sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

11. Kontroller og erklæringer

11.1 Leverandøren er forpligtet til at give Institutionen nødvendige oplysninger til, at Institutionen til enhver tid kan sikre sig, at Leverandøren overholder de krav, der følger af denne Aftale.

11.2 Institutionen, en repræsentant for Institutionen eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision, stille spørgsmål til og få udleveret dokumentation med henblik på at kontrollere, at Leverandøren overholder de krav, der følger af denne Aftale.

11.3 Leverandøren skal én gang årligt fremsende en erklæring til Institutionen om overholdelse af denne Aftale. Erklæringen skal udarbejdes i overensstemmelse med gældende anerkendte branchestandarder på området, og skal omfatte både Leverandørens og eventuelle underdatabehandleres databehandling. Den første erklæring skal foreligge senest 12 måneder efter indgåelse af nærværende databehandleraftale. Såfremt Institutionen ønsker en ekstern revisionserklæring, kan dette ske mod et vederlag.

11.4 I tilfælde af, at Institutionen og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en inspektion af de ovennævnte foranstaltninger i henhold til denne aftale, forpligter Leverandøren og Leverandørens underleverandører sig til at stille tid og ressourcer til rådighed herfor. Såfremt Institutionen vurderer, at der er behov for at anvende eksterne ressourcer i denne inspektion, så afholder Institutionen disse udgifter.

12. Ændringer i aftalen

I det omfang ændringer i lovgivningen, jf. pkt. 3.1 og 3.2, eller tilhørende praksis, giver anledning til dette, er Institutionen med et varsel på 60 dage og uden at dette medfører krav om betaling fra Leverandøren, berettiget til at foretage ændringer i Aftalen.

13. Sletning af data

13.1 Institutionen træffer beslutning om, hvorvidt der skal ske sletning af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt i medfør af "Købsaftalen", eller at der skal ske forsat opbevaring af personoplysninger med henblik på en fornyelse af "Købsaftalen" eller anden aftale om opbevaring af personoplysninger.

13.2 Institutionen skal senest 60 dage inden "Købsaftalens" ophør skriftligt meddele Leverandøren, hvorvidt alle personoplysningerne skal slettes eller fortsat opbevares. Leverandøren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever Institutionens meddelelse.

13.3 Leverandøren skal fremsende dokumentation for, at den påkrævede sletning, jf. pkt. 13.2, er foretaget.

14. Misligholdelse og tvistigheder

14.1 Misligholdelse og tvistigheder er reguleret i "Købsaftalen".

15. Ikrafttræden og varighed

15.1 Aftalen indgås ved begge parters underskrift og løber indtil et eventuelt ophør af kunderelationen mellem Leverandøren og Institutionen, jf. betingelserne i "Købsaftalen" eller "Købsaftalerne".

15.2 Opsigelse af indeværende aftale indebærer ikke en opsigelse af "Købsaftalen" eller "Købsaftalerne", eller at betalingsforpligtelsen jf. "Købsaftalen" eller "Købsaftalerne" bortfalder.

16. Formkrav

16.1 Aftalen skal foreligge skriftligt, herunder elektronisk, hos Institutionen og Leverandøren.

For Institutionen	For Leverandøren
Navn:	Navn:
Titel:	Titel:
Dato:	Dato:
_____	_____
Underskrift	Underskrift

Bilag 1 – Sikkerhed

1. Indledning

Dette bilag indeholder en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Leverandøren i medfør af Aftalen har ansvar for at gennemføre, overholde og sikre overholdelse af hos dennes underdatabehandlere, som er angivet i bilag 2.

2. Sikkerhedskrav indtil 25. maj 2018

Leverandøren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der opfylder kravene i Sikkerhedsbekendtgørelsen og tilhørende praksis.

Foranstaltningerne gennemføres for at undgå, at personoplysninger:

- tilintetgøres, mistes, ændres eller forringes,
- kommer til uvedkommendes kendskab eller misbruges,
- eller i øvrigt behandles i strid med lovgivningen, jf. Aftalens pkt. 3.1

Generelle sikkerhedsforanstaltninger
Clio Onlines IT-tekniske personale har adgang til personoplysninger med henblik på at udvikle, problemsøge, teste og fejlfinde i interne systemer i forhold til at optimere vores produkters performance og dermed understøtte formålet med databehandlingen. Dette sker via en sikret adgang med brugernavn og adgangskode. Der bliver ført tilsyn med disse adgangstilladelser og disse ajourføres jævnligt.

Wipping af datamedier

Når der opsættes brugte computere til nye medarbejdere bliver alt data og dataspor slettet. I forhold til Mac-computer anvendes det indbyggede diskværktøj til at slette hele partitionen på harddisken og geninstallerer styresystemet. I forhold til Windows computere anvendes den indbyggede 'Nulstil Windows' funktion, som ligeledes sletter alle partitioner på harddisken.

På harddiske, som skal ud af huset til destruktion, bliver alle sektorer på disken overskrevet med 0'er med Active Killdisk programmet.

Autorisation og adgangskontrol

Transfer af data mellem UNI-C og Clio Onlines systemer

Når en bruger vil benytte Clio Onlines produkter, omdirigeres brugeren til UNI•Login. UNI•Login autentificerer brugeren ved at identificere denne og dokumenterer over for Clio Onlines platform, hvem brugeren er. Efter denne autentifikation kontrollerer UNI•Login, om brugeren har abonnement til Clio Onlines produkter og sendes derefter ind i Clio Onlines produkt-univers. Hvis den pågældende institution, der har købt abonnement, ligeledes har tilmeldt sig dataaftalen via UNI-C, giver det Clio Onlines systemer mulighed for at indhente og lagre følgende oplysning:

- UNI-C brugernavn
- E-mail
- Navn
- Klassetilhørsforhold og institutionsnummer
- Funktion (Fx lærer, elev etc.)

Her kan du læse mere om, hvordan UNI•Login behandler personoplysninger:
https://viden.stil.dk/pages/viewpage.action?pageId=2360491

Fysisk datamiljø sikret efter Amazon web services høje standarder

Denne transfer af data fra UNI-C's systemer til Clio Onlines platform og database foregår via en krypteret forbindelse. Den overførte data bliver placeret i Clio Onlines fysiske datamiljø, der er sikret og adgangskontrolleret via *Amazon web services* (se bilag 2). *Amazon web services* er kendt for at have et af cloudløsningsmarkedets højeste sikkerhedsniveauer for databehandling, som uddybes her:

- https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf
- https://aws.amazon.com/compliance/

Adgang til datamiljø sikret via Bastion jump-server

Det fysiske datamiljø er sikret og adgangskontrolleret via Amazon web services. Det er udelukkende medarbejdere, der har et formål med at arbejde med de pågældende personoplysninger, der har fået kontrolleret adgang til disse systemer via brugernavn og kodeord. Selve adgangen til disse systemer foregår via en Bastion jump-server.

Inddatamateriale som indeholder personoplysninger

Udover den data, der bliver overført via sikrede forbindelse fra STIL og UNI•Login til Clio Onlines systemer, så bliver der også genereret andre typer af data. Det drejer sig overordnet om følgende data, som bliver registeret og lagret:

- Elevens resultater og besvarelser fra Opgavesystemet
- Elevens noter til læringsportalernes fagtekster

- Elevens svar og input i de interaktive elementer på læringsportaler
- Selvevaluering fra de interaktive forløb på læringsportal
- Sidevisninger og interaktion med produkterne

Ovenstående datatyper indhentes med henblik på at styrke mulighederne for at monitorere elevernes læringsprogression samt forbedre brugeroplevelsen. Dataen er lagret i et fysisk datamiljø, der er sikret og adgangskontrolleret via *Amazon web services* (se bilag 2).

Uddatamateriale som indeholder personoplysninger
Clio Onlines platform har et API (Application Programming Interface), der tillader at integrere andre typer af software med Clio Onlines, og dermed muliggør, at der kan overføres data mellem systemerne. Denne integration vil som hovedregel være med forskellige leverandører af LMS'ere (Learning Management Systems). I dette setup vil der foregå en autorisering af den uddata, der vil flyde fra Clio Onlines system og over i et LMS. Denne autorisation foregår ved, at læreren skal logge sig ind i LMS'et, som den pågældende skole anvender, og godkende, at elevdataen fra Clio Onlines systemer bliver overført til det pågældende LMS. Denne data bliver overført via en krypteret SSL-forbindelse.

Behandlingen af personoplysningerne over i det pågældende LMS er den pågældende leverandørs ansvar, hvorfor det er Institutionens ansvar at indhente en separat databehandleraftale med denne leverandør.

Eksterne kommunikationsforbindelser
Når der anvendes eksterne kommunikationsforbindelser ved tilslutning til Internettet, andre åbne net samt ved brug af interne webapplikationer sikrer Clio Online imod uvedkommende trafik og forhindrer adgang fra det åbne net via en firewall, som løbende kontrolleres og ajourføres. Det trådløse netværk er ligeledes sikret imod aflytning af kommunikationen og opsnappe brugeridentifikationer og dertil hørende fortrolige adgangskoder, som anvendes i forbindelse med autoriserede brugeres adgang til personoplysninger. Alt sammen ligger inde bag Network Layer Firewalls og Web Application Layer Firewalls (WAF).

Kontrol med afviste adgangsforsøg og logning
Det fremgår af sikkerhedsbekendtgørelsen § 15, at bestemmelserne i kapitel 3 om "kontrol med afviste adgangsforsøg" og "logning" ikke finder anvendelse i det omfang, de behandlede oplysninger ikke i sig selv ville være omfattet af anmeldelsespligten til Datatilsynet. Dette medfører, at når den behandling af personoplysninger, der skal finde sted, ikke kræver anmeldelse til Datatilsynet, gælder der ikke et krav om, at der skal foretages kontrol med afviste adgangsforsøg eller logning.

Ifølge persondataloven er der kun anmeldelsespligt, når en behandling vedrører fortrolige personoplysninger. Fortrolige oplysninger er f.eks. følsomme oplysninger, som angivet i persondataloven og databeskyttelsesforordningen, men fortrolige oplysninger kan også udstrækkes til andre oplysninger af rent privat karakter. Fortrolige oplysninger vil derfor også kunne være oplysninger om eksamenskarakterer, præstationer og bedømmelser.

Det følger imidlertid af bekendtgørelse om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for den offentlige forvaltning, at visse behandlinger er undtaget fra anmeldelsespligten. Her fremgår det af § 11, at behandlinger, som foretages i forbindelse med administration og planlægning af undervisning og ikke vedrører andet end eksamenskarakter og bedømmelser, ikke er omfattet af anmeldelsespligten.

Da behandlingen i Clio Online udelukkende omfatter behandling af ikke-fortrolige oplysninger eller oplysninger om bedømmelser i forbindelse med administration og planlægning af undervisning, er det ikke et krav at Clio Online foretager kontrol med afviste adgangsforsøg og logning.

Hjemmearbejdspladser
Clio Onlines behandling af personoplysninger sker delvist ved anvendelse af hjemmearbejdspladser. Hvis interne systemer tilgås fra en hjemmearbejdsplads, foregår det via krypterede VPN-forbindelser og tilgang til vores server-miljøer sker igennem en avanceret kryptografisk keybaseret forbindelse til vores fysiske datamiljø, der er sikret med *Amazon web services*.

Sikkerhedskrav fra 25. maj 2018

Leverandøren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger, jf. Instruks (bilag 3), og som dermed opfylder Databeskyttelsesforordningens artikel 32.

Foranstaltningerne fastlægges ud fra overvejelser om:

1. Hvad der kan lade sig gøre rent teknisk

2. Implementeringsomkostningerne

3. Den pågældende behandlings karakter, omfang, sammenhæng og formål, jf. Instruksen (bilag 3)

4. Konsekvenserne for borgerne ved et sikkerhedsbrud

5. Den risiko, der er forbundet med behandlingerne, herunder risikoen for:

    a) tilintetgørelse af oplysningerne

    b) tab af oplysningerne

    c) ændring af oplysningerne

    d) uautoriseret videregivelse af oplysningerne

    e) uautoriseret adgang til oplysningerne

De allerede beskrevne og implementerede tekniske og organisatoriske foranstaltninger vil efter 25. maj 2018 blive suppleret af en pseudonymisering og kryptering af personoplysningerne i Clio Onlines fysiske datamiljøer.

Bilag 2 – Oplysninger om lokationer for behandling og underleverandører (underdatabehandlere)

1. Lokation(er) for behandlingen

Clio Online
Esplanaden 8A, 1-2. Sal.
1263, København K
Danmark

2. Underdatabehandlere

Amazon web services
(Hosting)
One Burlington Plaza,
Burlington Road,
Dublin 4
Irland

Google Analytics
(Analytics tool)
1600 Amphitheatre Parkway
Mountain View, CA 94043
USA

Freshworks
(Freshdesk Support Tool)
1250 Bayhill Drive
Suite 315
San Bruno, CA 94066
USA

Ciklum
(IT test and development)
24, Soborna St
Sky Park, 3rd Floor, Office 4.218
Vinnytsia, 21050
Ukraine

Bilag 3 – Instruks

Instruks
Institutionen instruerer hermed Leverandøren om at foretage behandling af Institutionens oplysninger til brug for levering og drift af diverse digitale læremidler og hjælpemidler, herunder Læringsportaler, Opgavesystemet og Mit Clio, jf. Købsaftalen eller Købsaftalerne indgået mellem Clio Online og Institutionen.

Personoplysningerne behandles med henblik på at optimere produkternes performance og dermed forbedre muligheden for at monitorere elevprogression og styrke mulighederne for både lærerfeedback og selvevaluering hos den enkelte elev med henblik på at skabe den bedste læring. Institutionen og Institutionens lærere skal være opmærksom på, at Clio Online anvender udvalgte oplysninger til egne formål. Clio Online anvender f.eks. oplysninger om brugeradfærd til at kunne målrette den brugerorienterede dialog samt til at optimere vores produkter og tjenesteydelser. Clio Online vil derfor behandle udvalgte oplysninger i forbindelse med nyhedsbreve, markeds- og produktundersøgelser samt service- og produktorienteringer. Clio Online indsamler og registrerer selv disse oplysninger som dataansvarlig og er ansvarlig for, at denne behandling sker i overensstemmelse med persondataloven og databeskyttelsesforordningen.

Overlader Leverandøren behandling af Institutionens oplysninger til underdatabehandlere, er Leverandøren ansvarlig for at indgå skriftlige (under)databehandleraftaler med disse, jf. Aftalens pkt 6.3. Leverandøren er ansvarlig for, at Institutionens instruks fremsendes til eventuelle underdatabehandlere.

Leverandøren forpligter sig til udelukkende at anvende underdatabehandlere, der befinder sig i EU eller sikre tredjelande eller underleverandører der har underskrevet EU Kommissionens standardkontrakter for overførsel af personoplysninger til tredjelande. Leverandøren indestår således for, at de anvendte underdatabehandlere enten har tilsluttet sig EU-U.S. Privacy Shield ordningen eller har underskrevet EU Kommissionens standardkontrakter for overførsel af personoplysninger til tredjelande.

1.1 Behandlingens formål

Behandling af Institutionens oplysninger sker i henhold til formålet i Aftalen.

Leverandøren må ikke anvende oplysningerne til andre formål end beskrevet i instruksen.

Oplysningerne må ikke behandles efter instruks fra andre end Institutionen.

1.2 Generel beskrivelse af behandlingen

Leverandøren instrueres af Institutionen til at håndtere og behandle personoplysninger med særligt henblik på at styrke mulighederne for at monitorere elevernes læringsprogression, give og dokumentere lærerfeedback samt styrke mulighederne for, at eleven kan foretage selvevaluering. Leverandøren instrueres i den forbindelse af Institutionen til at foretage profilering af de registrerede, som defineret ved databeskyttelsesforordningens artikel 4, nr. 4, udelukkende til de formål som er beskrevet i instruksen. Denne databehandling vil foregå indtil et eventuelt ophør af kunderelationen mellem Leverandøren og Institutionen, jf. "Købsaftalen" eller "Købsaftalerne".

1.3 Typen af personoplysninger

Behandlingerne indeholder personoplysninger i de nedenfor afkrydsede kategorier. Leverandørens og eventuelle underdatabehandleres niveau for behandlingssikkerhed bør afspejle oplysningernes følsomhed, jf. bilag 1.

Almindelige personoplysninger (indtil 25. maj 2018, jf. Persondatalovens § 6, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 6)

☒ Almindelige personoplysninger

Følsomme personoplysninger (indtil 25. maj 2018, jf. Persondatalovens § 7, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 9):

☐ Racemæssig eller etnisk baggrund
☐ Politisk overbevisning
☐ Religiøs overbevisning
☐ Filosofisk overbevisning
☐ Fagforeningsmæssige tilhørsforhold
☐ Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol m.v.
☐ Seksuelle forhold

Oplysninger om enkeltpersoners rent private forhold (indtil 25. maj 2018, jf. Persondatalovens § 8, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 6 og 9):

☐ Strafbare forhold
☐ Væsentlige sociale problemer
☒ Andre rent private forhold, som ikke er nævnt ovenfor:

Oplysninger om præstation, bedømmelser, evalueringer, læringsprogression.

Oplysninger om cpr-nummer (indtil 25. maj 2018, jf. Persondatalovens § 11, fra 25. maj 2018, eventuelt national lovgivning, jf. Databeskyttelsesforordningens artikel 87)

☐ CPR-numre

1.4 Kategorier af registrerede

Der behandles oplysninger om følgende kategorier af registrerede (f.eks. borgere, elever, kontanthjælpsmodtagere m.m.):

A) Lærer og andet uddannelsespersonale i grundskole.

B) Elever på klassetrinnene 0.-10.klasse.