

DATABEHANDLERAFTALE

Mellem

Haslev Privatskole
Haslev
Institutionsnr. 313007
(herefter "Skolen")

og

JH Software Aps
Vesteråsene 34
9900 Frederikshavn
CVR. nr.: 28867077
(herefter "JH Software")

er der indgået nedenstående databehandleraftale (herefter "Aftalen") om JH Softwares
behandling af personoplysninger på vegne af Skolen:

1. Generelt

1. Aftalen vedrører JH Softwares 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:
 1. Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsbekendtgørelsen).
 2. 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).
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 (1.1.1) – (1.1.2) herefter erstattes med Databeskyttelsesforordningen.
3. I Aftalen er indarbejdet de krav, som såvel Persondataloven som de kommende regler i Databeskyttelsesforordningen stiller til databehandleraftaler.
4. JH Software skal behandle personoplysninger i overensstemmelse med god databehandlingsskik, jf. de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

2. Formål

JH Software udvikler og udgiver Tjek web-stederne (Biologi-Tjek, Geografi-Tjek, Fysik-Kemi-Tjek, Natur-Teknologi-Tjek, m.fl.) henvendt til grundskolen. Webstederne indeholder primært emneopdelte trænings- og test-opgaver, som i layout og indhold ligner de digitale afgangsprøver og nationale test. Se <http://tjek.net>

JH Software behandler personoplysninger for Skolen når Skolen tegner abonnement(er) på et eller flere af Tjek web-stederne.

3. Skolens rettigheder og forpligtelser

1. Skolen er dataansvarlig for de personoplysninger, som Skolen instruerer JH Software om at behandle. Skolen har ansvaret for, at de personoplysninger, som Skolen instruerer JH Software om at behandle, må behandles af JH Software, herunder at behandlingen er nødvendig og saglig i forhold til Skolens opgavevaretagelse.
2. Skolen har de rettigheder og forpligtelser, som er givet en dataansvarlig i medfør af lovgivningen, jf. Aftalens pkt. 1.1 og 1.2.

4. JH Softwares forpligtelser

1. JH Software er databehandler for de personoplysninger, som JH Software behandler på vegne af Skolen, jf. pkt. 6 og bilag 3. JH Software har som

databehandler de forpligtelser, som er pålagt en databehandler i medfør af lovgivningen, jf. Aftalens pkt. 1.1 og 1.2.

2. JH Software behandler alene de overladte personoplysninger efter instruks fra Skolen, jf. pkt. 6 og bilag 3, og alene med henblik på at Skolens elever og lærere kan anvende Tjek web-stederne.
3. JH Software skal fra 25. maj 2018 løbende føre en fortegnelse over behandlingen af personoplysninger samt en fortegnelse over alle sikkerhedsbrud.
4. JH Software 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. JH Software skal på opfordring fra Skolen hjælpe med at opfylde Skolens 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 Skolens forpligtelser i forhold til underretning af den registrerede ved sikkerhedsbrud, fra 25. maj 2018 i medfør af Databeskyttelsesforordningens kap. III samt artikel 34.
6. JH Software skal fra 25. maj 2018 hjælpe Skolen med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens artikel 32-36.
7. JH Software garanterer fra 25. maj 2018 at levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger sådan, at JH Softwares behandling af Skolens personoplysninger opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.
8. Hvis JH Software er etableret i en anden EU-medlemsstat, skal JH Software frem til 25. maj 2018 ligeledes overholde de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat.

5. Underleverandør (underdatabehandler)

1. Ved underdatabehandler forstås en underleverandør, til hvem JH Software har overladt hele eller dele af den behandling, som JH Software foretager på vegne af Skolen.
2. JH Software har ret til at anvende andre underdatabehandlere end dem, som er angivet i bilag 2, til at behandle de personoplysninger, som Skolen har overladt til JH Software. JH Software skal ajourføre oplysninger om underdatabehandlere i bilag 2 ved enhver ændring. Skolen kan ikke nægte at godkende tilføjelse eller udskiftning af en underdatabehandler medmindre, der foreligger en konkret saglig begrundelse herfor.
3. Hvis JH Software overlader behandlingen af personoplysninger, som Skolen er dataansvarlig for, til underdatabehandlere, skal JH Software indgå en skriftlig (under)databehandleraftale med underdatabehandleren.

4. Underdatabehandleraftalen, jf. pkt. 5.3, skal pålægge underdatabehandleren de samme databeskyttelsesforpligtelser, som JH Software 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.
5. Når JH Software overlader behandlingen af personoplysninger, som Skolen er dataansvarlig for, til underdatabehandlere, har JH Software over for Skolen ansvaret for underdatabehandlernes overholdelse af disses forpligtelser, jf. pkt. 5.3.
6. Skolen kan til enhver tid forlange dokumentation fra JH Software for eksistensen og indholdet af underdatabehandleraftaler for de underdatabehandlere, som JH Software anvender i forbindelse med opfyldelsen af sine forpligtelser over for Skolen.
7. Al kommunikation mellem Skolen og underdatabehandleren sker via JH Software.

6. Instrukser

1. JH Softwares behandling af personoplysninger på vegne af Skolen sker udelukkende efter dokumenteret instruks, jf. bilag 3. Det er JH Softwares ansvar at sikre, at eventuelle underdatabehandlere, jf. pkt 5.3, får tilsendt Skolens instruks, jf. bilag 3.
2. JH Software giver fra 25. maj 2018 omgående besked til Skolen, hvis en instruks efter JH Softwares vurdering er i strid med lovgivningen, jf. pkt. 1.2.

7. Tekniske og organisatoriske sikkerhedsforanstaltninger

1. JH Software skal frem til 25. maj 2018, jf. bilag 1, træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger:
 - tilintetgøres, mistes, ændres eller forringes,
 - kommer til uvedkommendes kendskab eller misbruges, eller
 - i øvrigt behandles i strid med lovgivningen, jf. pkt. 1.1.
2. JH Software skal fra 25. maj 2018, jf. bilag 1, iværksætte alle sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.
3. JH Software 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. 7.1 og 7.2, samt bilag 1.
4. JH Software samt dennes ansatte er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.

5. JH Software har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af Skolens personoplysninger, om JH Softwares forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed, jf. pkt 9.
6. JH Software er forpligtet til straks at underrette Skolen om ethvert sikkerhedsbrud uanset, om dette sker hos JH Software eller hos en underdatabehandler.

8. Overførsler til andre lande

1. JH Software må ikke overføre personoplysninger til lande, der ikke er medlem af EU (tredjelande).
2. Hvis Skolens personoplysninger overføres til en EU-medlemsstat, er det frem til 25. maj 2018 JH Softwares ansvar, at de til enhver tid gældende bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat, overholdes.

9. Tavshedspligt og fortrolighed

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

10. Kontroller og erklæringer

1. JH Software er forpligtet til at give Skolen nødvendige oplysninger til, at Skolen til enhver tid kan sikre sig, at JH Software overholder de krav, der følger af denne Aftale.
2. Skolen, en repræsentant for Skolen eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision hos JH Software, med henblik på at konstatere, at JH Software overholder de krav, der følger af denne Aftale.
3. JH Software skal én gang årligt vederlagsfrit til Skolen fremsende en erklæring om overholdelse af denne Aftale. Erklæringen skal udarbejdes i overensstemmelse med gældende, anerkendte branchestandarder på området, og skal omfatte både JH Softwares og eventuelle underdatabehandlers databehandling. Den første erklæring skal foreligge 12 måneder efter aftalens indgåelse.
4. I tilfælde af, at Skolen og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en inspektion af de ovennævnte foranstaltninger i henhold til denne aftale, forpligter JH Software og JH Softwares underleverandører sig til uden yderligere omkostninger for Skolen at stille tid og ressourcer til rådighed herfor.

11. Ændringer i Aftalen

1. I det omfang ændringer i lovgivningen, jf. pkt 1.1 og 1.2, eller tilhørende praksis, giver anledning til dette, er Skolen med et varsel på 60 dage og uden at dette medfører krav om betaling fra JH Software, berettiget til at foretage ændringer i Aftalen.

12. Sletning af data

1. Skolen træffer beslutning om, hvorvidt der skal ske sletning af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt i medfør af udløbet af abonnement, eller at der skal ske fortsat opbevaring af personoplysninger med henblik på en fornyelse af abonnement.
2. JH Software skal slette alle personoplysninger senest et år efter ophørt abonnement (det meste data slettes umiddelbart efter endt abonnement, men nogle data gemmes op til et år med henblik på gen-aktivering af abonnement). JH Software skal sikre, at eventuelle underdatabehandlere ligeledes sletter data.
3. Skolen skal skriftligt meddele JH Software, hvis personoplysningerne skal slettes tidligere end 1 år efter udløb af abonnement. JH Software skal sikre, at eventuelle underdatabehandlere ligeledes efterlever Skolens meddelelse.

13. Ikrafttræden og varighed

1. Aftalen indgås ved begge parter underskrift og løber indtil den skriftligt opsiges af en af parterne.
2. Aftalen kan opsiges af begge parter med 60 dages varsel.
3. Ved opsigelse skal der enten indgås en ny databehandleraftale, eller JH Software skal slette alle personoplysninger opbevaret for Skolen senest 60 dage efter opsigelsen.

14. Formkrav

1. Aftalen skal foreligge skriftligt, herunder elektronisk, hos Skolen og JH Software.

For Haslev Privatskole

Dato: 15.2.2018

Lisbeth Trap Nyholt

Underskrevet elektronisk:

E-mail: adm@haslevprivatskole.dk

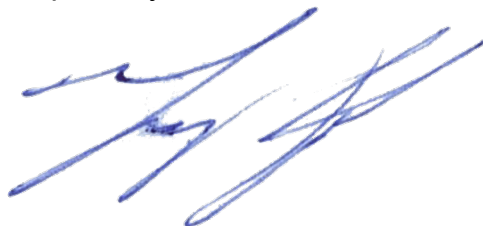
IP adresse: 5.103.128.249

Tid: kl. 08:48:51

For JH Software

Dato: 15.2.2018

Jesper Høy



Bilag:

- Bilag 1 – Sikkerhed
- Bilag 2 – Oplysninger om lokationer for behandling og underleverandører (underdatabehandlere)
- Bilag 3 – Instruks

Bilag 1 – Sikkerhed

1. Indledning

Dette bilag indeholder en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som JH Software 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

JH Software 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. 1.1

Generelle sikkerhedsforanstaltninger

Personoplysninger, som behandles af JH Software for Skolen, eksisterer primært på JH Softwares web-servere som er hostet ved Amazon Web Services (se bilag 2).

Amazon Web Services er kendt for at have et af markedets højeste sikkerhedsniveauer for databehandling, hvilket uddybes her:

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

Det er udelukkende JH Softwares medarbejdere, der har et formål med at arbejde med de pågældende personoplysninger, der har adgang til disse web-servere.

JH Softwares 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 krypteret og sikret adgang med brugernavn og adgangskode. Der bliver ført tilsyn med disse adgangstilladelser og disse ajourføres jævnligt.

JH Softwares lokale dataudstyr repareres og serviceres kun internt og kun af eget personale.

På harddiske, som skal ud af huset til destruktion, bliver hele harddisken først overskrevet med tilfældig data med CBL Data Shredder programmet.

Når der opsættes brugte computere til nye medarbejdere bliver alt data først slettet ved først at overskrive hele harddisken med tilfældig data med CBL Data Shredder programmet. Derefter installeres styresystem og applikationer på ny.

Autorisation og adgangskontrol

Ved brug af JH Softwares Tjek websteder, kan en institution vælge at anvende enten UNI-Login eller selvvalgte brugernavne/adgangskoder til autorisation/adgangskontrol for lærere og elever.

- For institutioner som vælger at bruge UNI-Login:

Når en bruger vil benytte et af JH Softwares Tjek websteder, omdirigeres brugeren til UNI-Login. UNI-Login autentificerer brugeren ved at identificere denne og dokumenterer over for JH Softwares web-server, hvem brugeren er (UNI-Login bruger-ID). Ud fra det angivne bruger-ID indhenter og lagrer JH Softwares web-server så brugerens institutions-tilknytning(er) inkl. institutionsnr. og funktioner (lærer, elev, etc.) fra UNI-Login. og kontrollerer om institutionen har et abonnement på web-stedet, og om brugeren har adgang til dette. Hvis den pågældende institution har tilmeldt sig dataaftalen via UNI-Login, giver det endvidere JH Softwares systemer mulighed for at indhente og lagre navn og (for elever) klasse/hold-tilhørsforhold fra UNI-Login. Har institutionen ikke tilmeldt sig dataaftalen, bedes brugeren angive navn og klasse/hold ved første login.

Overførsel af data fra UNI-Login til JH Softwares web-server foregår via en krypteret forbindelse.

JH Software har IKKE adgang til brugernes adgangskoder.

For information om hvordan UNI-Login behandler personoplysninger, se <https://viden.stil.dk/pages/viewpage.action?pageId=2360491>

- For institutioner som vælger at bruge selvvalgte brugernavne/adgangskoder:

For alle brugere er autorisation / adgang kontrolleret ved hjælp af brugernavn og adgangskode.

Adgangskoder er lagret i en en-vejs-krypteret form (SHA-1 hash værdi) og forefindes ikke i klartekst. De kan derfor ikke ses af hverken JH Softwares medarbejdere eller andre, der måtte få adgang til bruger-databasen.

Inddatamateriale som indeholder personoplysninger

Udover data, der evt. bliver overført fra UNI-Login til JH Softwares systemer (se ovenfor), så bliver der også genereret andre typer af data. Det drejer sig overordnet om følgende data, som bliver registeret og lagret:

- Elevers resultater og besvarelser af opgavesæt.
- Beskeder fra lærere til elever.
- Læreres/elevs navne (fra UNI-Login eller indtastet)
- Læreres/elevs e-mail adresser - hvis man vælger at bruge disse som bruger-ID til login.
- Læreres e-mail adresser - hvis de vælger at oplyse dem til notifikations-formål.
- Logning af tidspunkt og IP-adresse ved login.

Ovenstående datatyper indhentes for at understøtte funktionaliteten af webstederne, for at muliggøre monitorering af elevernes læringsprogression, samt forbedre brugeroplevelsen.

Personoplysninger slettes senest et år efter ophørt abonnement (det meste data slettes umiddelbart efter endt abonnement, men nogle data gemmes op til et år med henblik på gen-aktivering af abonnement). Alle oplysninger slettes med det samme, hvis Skolen skriftligt anmoder JH Software om dette.

Uddatamateriale som indeholder personoplysninger

JH Software har til hensigt at tilbyde integration med diverse lærings-portal-systemer. Denne integration vil som hovedregel være med forskellige leverandører af systemer baseret på Bruger Portal Initiativet. I en sådan integration vil der foregå en autorisering af den uddata, der vil flyde fra JH Softwares system og over i en sådan portal. Denne autorisation vil foregå ved, at læreren skal logge sig ind i portalen som den pågældende institution anvender, og godkende, at elevdata fra JH Softwares systemer bliver overført til den pågældende portal. Disse data vil blive overført via en krypteret SSL-forbindelse. Behandlingen af personoplysningerne over i den pågældende portal vil være den pågældende leverandørs ansvar, hvorfor det er kommunens/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 JH Software sig imod uvedkommende trafik og forhindrer adgang fra det åbne net via en firewall, som løbende kontrolleres og ajourføres. Trådløse netværk er ligeledes sikret imod indtrængning og aflytning.

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 ved JH Software 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 JH Software foretager kontrol med afviste adgangsforsøg og logning.

Hjemmearbejdspladser

JH Softwares behandling af personoplysninger sker helt eller delvist ved anvendelse af hjemmearbejdspladser.

Når interne systemer tilgås fra en hjemmearbejdsplads, foregår det via krypterede VPN-forbindelser.

Adgang til personoplysninger på web-server foregår via krypteret forbindelse (SSL) til administrations-websted beskyttet med bruger-id og adgangskode.

3. Sikkerhedskrav fra 25. maj 2018

JH Software 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

JH Software opfylder databeskyttelsesforordningens artikel 32 (se stk. 1, litra b) ved at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester gennem følgende tiltag:

- Fortrolighed: Se afsnit om "Generelle sikkerhedsforanstaltninger" og "Autorisation og adgangskontrol" under punkt 2 ovenfor.
- Integritet: Nøjagtighed og fuldstændighed af persondata (lagret i en Microsoft SQL database) kontrolleres løbende med værktøjet "checkdb" (checksum kontrol).
- Tilgængelighed: Persondata lagres på dublerede diske (Amazon Elastic Block Store - se <https://aws.amazon.com/ebs>), og der laves automatisk daglig backup af komplet database fra web-server (i Amazons datacenter) til JH Softwares hovedkontor.
- Robusthed: Der anvendes dublerede diske, køling, nødstrømsanlæg, automatisk brandslukning, mv. i Amazons datacentre - se <https://aws.amazon.com/compliance/data-center/infrastructure-layer>

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

1. Lokation(er) for behandlingen:

JH Software ApS
Vesteråsene 34
9900 Frederikshavn
Danmark
CVR-Nr. 28867077

2. Underdatabehandlere:

Amazon Web Services
Frankfurt
Tyskland

Se <https://aws.amazon.com>

(Amazon oplyser ikke præcise adresser på datacentre grundet sikkerhedshensyn)

Bilag 3 – Instruks

Instruks

Skolen instruerer hermed JH Software om at foretage behandling af Skolens oplysninger til brug for drift/levering af Tjek webstederne (se <http://tjek.net>).

Overlader JH Software behandling af Skolens oplysninger til underdatabehandlere, er JH Software ansvarlig for at indgå skriftlige (under)databehandleraftaler med disse, jf. Aftalens pkt 5.3. JH Software er ansvarlig for, at Skolens instruks fremsendes til eventuelle underdatabehandlere.

1. Behandlingens formål

Behandlingen af Skolens oplysninger sker for at Skolens elever og lærere kan anvende Tjek web-stederne (se <http://tjek.net>).

JH Software må ikke anvende oplysningerne til andre formål.

Oplysningerne må ikke behandles efter instruks fra andre end Skolen.

2. Generel beskrivelse af behandlingen

Behandling af Skolens oplysninger sker primært for at identificere elever og deres handlinger overfor lærere på Tjek web-stederne. F.eks. således at en lærer kan se hvilke elever der har besvaret et opgavesæt og hvordan.

Elevers og læreres e-mail adresser (hvis oplyst) bruges til administrative forhold (f.eks. ændring af adgangskode), notifikation om abonnement-forhold og evt. nyheder iht. aftale med den enkelte bruger.

Oplysningerne bruges også til at identificere elever og lærere overfor JH Software til support-formål.

JH Software anvender udvalgte anonymiserede oplysninger til egne formål, f.eks. oplysninger om brugeradfærd til at kunne optimere Tjek web-stederne.

3. Typen af personoplysninger

Behandlingerne indeholder **kun almindelige personoplysninger** (indtil 25. maj 2018, jf. Persondatalovens § 6, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 6)

Behandlingerne indeholder **IKKE følsomme personoplysninger** (indtil 25. maj 2018, jf. Persondatalovens § 7, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 9)

Behandlingerne indeholder **IKKE oplysninger om enkeltpersoners rent private forhold** (indtil 25. maj 2018, jf. Persondatalovens § 8, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 6 og 9)

Behandlingerne indeholder **IKKE oplysninger om cpr-nummer** (indtil 25. maj 2018, jf. Persondatalovens § 11, fra 25. maj 2018, eventuelt national lovgivning, jf. Databeskyttelsesforordningens artikel 87)

4. Kategorier af registrerede

Der behandles oplysninger om følgende kategorier af registrerede:

- Elever på uddannelsesinstitutioner (primært grundskole)
- Lærere og andet uddannelsespersonale på uddannelsesinstitutioner (primært grundskole)

5. Tredjelande (ikke EU-medlemslande)

JH Software må **IKKE** overføre personoplysninger til tredjelande.