Standardkontraktsbestemmelser

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

mellem

Eksempel Skole/Kommune
CVR 12345678
Eksempel adresse
1234 Eksempel By
Danmark

herefter ”den dataansvarlige”

og

JH Software ApS
CVR 28867077
Vesteråsene 34
9900 Frederikshavn
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

2. Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.
2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).
3. I forbindelse med leveringen af Tjek.net webstederne (se https://tjek.net) behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.
4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.
10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes 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 beskyttelsesniveau, der passer til disse risici.

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

   a. Pseudonymisering og kryptering af personoplysninger
   b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
   c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
   d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.
3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

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

7. Anvendelse af underdatabehandlere

1. Databehandleren må IKKE anvende underdatabehandlere.

8. Overførsel til tredjelande eller internationale organisationer

1. Databehandleren må IKKE overføre personoplysningen til tredjeland eller internationale organisationer.

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 nærmeret angivet i Bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

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

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.
3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.
4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.
5. Underskrift

   På vegne af den dataansvarlige

Navn	Eksempel Navn
Stilling	Eksempel Stilling
Telefonnummer	11223344
E-mail	eksempel@eksempel.dk

   Underskrevet elektronisk:
   IP adresse: 12.13.14.15
   Tid: kl. 00:33:47 d. 18.6.2024

   _____
   Underskrift

   På vegne af databehandleren

Navn	Jesper Høy
Stilling	Direktør
Telefonnummer	71 78 53 34
E-mail	support@tjek.net

   

   18.6.2024

   _____
   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	Eksempel Navn
Stilling	Eksempel Stilling
Telefonnummer	11223344
E-mail	eksempel@eksempel.dk

Navn	Jesper Høy
Stilling	Direktør
Telefonnummer	71 78 53 34
E-mail	support@tjek.net

Bilag A - Oplysninger om behandlingen

Databehandleren udvikler og udgiver Tjek web-stederne (Biologi-Tjek, Geografi-Tjek, Fysik-Kemi-Tjek, Matematik-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 https://tjek.net. Databehandleren behandler personoplysninger for dataansvarlig når dataansvarlig tegner abonnement(er) på et eller flere af Tjek web-stederne.

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

Behandlingerne har til formål at muliggøre varetagelsen af dataansvarligs opgaver i forhold til at fremme børn og unges udvikling og læring - gennem anvendelse af Tjek web-stederne.

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

Behandling af personoplysninger sker primært for at identificere elever og deres handlinger over for 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 databehandleren til support-formål.

Lærere og elever oprettes som brugere på databehandlerens Tjek-websteder, enten via invitations-links, eller automatisk ved første log ind med Uni-Login.

Ved automatisk oprettelse af Uni-Login-brugere kontrolleres institutions-tilknytning og rolle (lærer/elev) via Uni-Login webservice ("ws71/wsiBRUGER" / hentBrugersInstitutionstilknytninger). Der indhentes IKKE yderligere oplysninger om lærere/elever fra Uni-Login.

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

Behandlingen omfatter kun almindelige personoplysninger (jf. Databeskyttelsesforordningens artikel 6).

Behandlingen omfatter IKKE følsomme personoplysninger (jf. Databeskyttelsesforordningens artikel 9), oplysninger om enkeltpersoners rent private forhold (jf. Databeskyttelsesforordningens artikel 6 og 9) eller oplysninger om cpr-nummer (eventuelt national lovgivning, jf. Databeskyttelsesforordningens artikel 87).

Specifikt behandles følgende personoplysninger:

- Læreres/elevers navne
- Læreres/elevers login-ID
- Elever og læreres e-mail adresser - hvis de vælger at oplyse dem til login- eller notifikations-formål
- Logning af tidspunkt og IP-adresse ved login
- Elevers resultater og besvarelser af opgavesæt
- Beskeder fra lærere til elever

A.4. Behandlingen omfatter følgende kategorier af registrerede

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

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

Behandlingen følger normalt skoleåret (august til juni). Alle abonnementdata (inkl. personoplysninger) slettes hos databehandleren hvert år i juli. Ved fornyelse af abonnement (for en skole), fortsætter behandlingen yderligere et skoleår (med nye personoplysninger). Dataansvarlig dog kan til enhver til opsige abonnement og anmode om sletning af personoplysninger med en uges varsel.

Bilag B - Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ingen (der må ikke anvendes underdatabehandlere jf. pkt. 7).

B.2. Varsel for godkendelse af underdatabehandlere

Ikke relevant (der må ikke anvendes underdatabehandlere jf. pkt. 7).

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:

Behandler, opbevarer, fremviser data indtastet / angivet af elever og lærere i forbindelse med deres brug af Tjek-webstederne - jf. bilag A.

Dette omfatter oprettelse og administration af lærere/elever, læreres beskeder til elever, læreres åbning af test-opgavesæt til besvarelse, elevers besvarelse af trænings og test-opgavesæt, læreres visning af opsummerede og individuelle test-resultater, mv.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Ud fra typen af personoplysninger som behandles (kun almindelige personoplysninger - se A.3), vurderes de konsekvenser der evt. kan være for de registrerede ved datatab eller datalæk, ikke at foranledige et særligt sikkerhedsniveau.

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:

- Ved enhver form for transmission af personoplysninger over Internettet samt over databehandlers lokalnetværk, anvendes kryptering (TLS/SSL).
  Personoplysninger pseudonymiseres så vidt muligt - f.eks. I databehandlers administrative systemer, hvor personoplysninger kun fremgår når det er absolut nødvendigt, og da kun for autoriseret personale.
- Vedvarende fortrolighed, integritet, tilgængelighed, samt robusthed af behandlingssystemer og tjenester, sikres som følger:
  - **Fortrolighed:**
    Personoplysninger, som behandles af databehandleren for dataansvarlig, eksisterer primært på databehandlerens web-server som er fysik placeret i et aflåst lokale på databehandlerens egen adresse.
    Det er udelukkende databehandlerens medarbejdere, der har et formål med at arbejde med de pågældende personoplysninger, der har adgang til denne web-server.
    databehandlerens 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.
    Databehandlerens 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.
    Til autorisation/adgangskontrol af lærere og elever på databehandlerens Tjek-websteder anvendes 3. parts login-leverandører (herunder Uni-Login, Microsoft-konto og Google-konto) eller log ind med e-mail og adgangskode. Dataansvarlig kan (via Tjek-websted eller striftlig instruks) begrænse dette til en eller flere specifikke leverandører / metoder pr. abonnement.
    Ved log ind med 3. parts login-leverandør opbevarer Databehandleren ikke læreres og elevers adgangskoder (hverken i klar tekst eller krypteret), da dette er overladt til login-leverandøreren.
    Ved log ind med e-mail og adgangskode, opbevarer Databehandleren kun en hash-værdi (SHA2 eller bedre, salted, mv.) af læreres og elevers adgangskoder, og har dermed ikke adgang til selve adgangskoden.
  - **Integritet:**
    Nøjagtighed og fuldstændighed af persondata (lagret i en lokal Microsoft SQL database) kontrolleres løbende med værktøjet "checkdb" (checksum kontrol).
  - **Tilgængelighed:**
    Der laves automatisk daglig backup af komplet database.
  - **Robusthed:**
    Web-server og Internet-router er forbundet til nødstrømsanlæg (UPS).

  Der anvendes desuden firewall (hardware og software) samt anti-virus software.
- Rettidig genopretning af tilgængelighed og adgang til personoplysninger i tilfælde af en fysisk eller teknisk hændelse, sikres gennem backup, standby systemer, mv.
- Der foretages regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden.
- Adgang til personoplysninger via Internettet, sikres via adgangskontrol (login) samt SSL kryptering.
- Personoplysninger beskyttes under transmission via SSL kryptering.
- Personoplysninger beskyttes under opbevaring via fysisk sikring samt netværksbeskyttelse (firewall mm.)
- Lokaliteter hvor der behandles personoplysninger sikres fysisk ved aflåsning.
- Ved anvendelse af hjemmearbejdspladser tilgås personoplysninger på web-server via krypteret forbindelse (SSL) til administrations-websted beskyttet med bruger-id og adgangskode. Personoplysninger opbevares IKKE på lokale enheder,

computere mv.
- Tidspunkt og IP-adresse logges ved log ind.

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:

Som en integreret del af Tjek-webstederne kan dataansvarligs ansatte (lærere / administrativt personale) selv fremsøge, opdatere, og slette alle personoplysninger opbevaret ved databehandleren.
Dette kan anvendes af dataansvarlig ved anmodninger i forbindelse med registreredes ret til indsigt, berigtigelse, sletning, begrænsning af behandling, samt indsigelse (jf. 9.1.c/d/e/f/g/i).

I forhold til registreredes "ret til oplysning" - ved første registrering oplyser databehandler de registrerede om hvad behandlingen indbefatter, herunder hvorfor personoplysningerne behandles, hvor længe de vil blive behandlet, og at vi behandler oplysningerne på vegne af dataansvarlig (jf. 9.1.a/b)

I forhold til registreredes "ret til dataportabilitet", er der ikke nogen personoplysninger under denne aftale, som teknisk set kan porteres eller som det ville give mening at portere (jf. 9.1.h).

I forhold til registreredes "ret til ikke at være genstand for en automatisk afgørelse", gør databehandleren specifikt opmærksom på at elevers test-resultater på Tjek-webstederne IKKE bør stå alene i standpunktsvurderinger af den enkelte elev (jf. 9.1.j).

Databehandleren vil informere dataansvarlig om ethvert brud på persondatasikkerheden uden unødig forsinkelse og om muligt senest 24 timer efter at databehandleren er blevet bekendt med det (jf. 9.2.a/b).

Databehandleren har foretaget en konsekvensanalyse vedrørende databeskyttelse. Denne viser at behandlingen IKKE vil føre til en høj risiko. Derfor er der ikke belæg for at høre en tilsynsmyndighed (jf. 9.2.c/d).

C.4 Opbevaringsperiode/sletterutine

Behandlingen følger normalt skoleåret (august til juni).

Alle abonnement-data (inkl. personoplysninger) slettes hos databehandleren hvert år i juli. Indgås aftale om forlængelse af abonnement, vil data stadig blive slettet i juli og aftalen påbegyndes på ny med nye personoplysninger.

Dataansvarlig kan dog til enhver tid opsige abonnement og anmode om sletning af personoplysninger med en uges varsel.

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:

JH Software ApS
Vesteråsene 34
9900 Frederikshavn

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Databehandleren må ikke overføre personoplysninger til tredjelande eller internationale organisationer.

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

Databehandleren skal en gang årligt vederlagsfrit til den dataansvarlige fremsende en erklæring om overholdelse af denne aftale. Den første erklæring skal foreligge senest 12 måneder efter aftalens indgåelse.

Ovennævnte erklæring vedhæftes en intern inspektionsrapport vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse bestemmelser.

Den dataansvarlige kan stille opfølgende spørgsmål i form af spørgeskema eller lignende, hvilket databehandleren skal besvare uden nødig forsinkelse.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt.

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

Ikke relevant, da der må ikke anvendes underdatabehandlere jf. pkt. 7.

Bilag D - Parternes regulering af andre forhold

Behandling

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

Den dataansvarliges rettigheder og forpligtelser

- Den dataansvarlige har ansvaret for, at de personoplysninger, som den dataansvarlige instruerer databehandleren om at behandle, må behandles af databehandleren, herunder at behandlingen er nødvendig og legitim i forhold til den dataansvarliges opgavevaretagelse.

Databehandleren handler efter instruks

- Databehandleren har de forpligtelser, som er pålagt en databehandler i medfør af lovgivningen, jf. Bestemmelsernes pkt. 2.2.
- Databehandleren skal føre fortegnelser over behandlingen af personoplysninger samt fortegnelser over alle brud på persondatasikkerheden.
- Databehandleren er forpligtet til at oplyse med præcise adresseangivelser, hvor Den dataansvarliges personoplysninger behandles, jf. bilag C,C.5. Databehandleren skal ajourføre oplysningerne over for den dataansvarlige ved enhver ændring.

Fortrolighed

- Databehandleren er - under og efter Hovedaftalens ophør - pålagt fuld tavshedspligt omkring alle oplysninger, denne bliver bekendt med gennem samarbejdet. Bestemmelserne indebærer, at tavshedspligtsbestemmelserne i straffelovens §§ 152-152f, jf. straffelovens § 152a, finder anvendelse.
- Databehandleren samt dennes ansatte er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.
- Databehandleren må ikke hverken offentligt eller til tredjeparter kommunikere om brud på persondatasikkerheden, jf. pkt 10.1 uden forudgående skriftlig aftale med den dataansvarlige om indholdet af en sådan kommunikation, medmindre databehandleren har en retlig forpligtelse til sådan kommunikation.

Behandlingssikkerhed

- Databehandleren 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. C,C.2.
- Databehandleren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af den dataansvarliges personoplysninger, om databehandlerens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed, jf. pkt 5.
- Databehandleren er forpligtet til uden unødig forsinkelse at underrette den dataansvarlige om
    i. enhver anmodning om videregivelse af personoplysninger omfattet af Bestemmelserne fra en myndighed, medmindre orienteringen af den dataansvarlige er eksplicit forbudt ved lov, f.eks. i medfør af regler, der har til formål at sikre fortroligheden af en retshåndhævende myndigheds efterforskning,
    ii. anden manglende overholdelse af databehandlerens, samt eventuelle underdatabehandleres forpligtelser uanset, om dette sker hos databehandleren eller hos en underdatabehandler.

Revision, herunder inspektion

- Databehandleren er forpligtet til uden ugrundet ophold at give den dataansvarlige de nødvendige oplysninger til, at den dataansvarlige til enhver tid kan sikre sig, at databehandleren overholder de krav, der følger af disse Bestemmelser.
- I forbindelse med revisioner, herunder inspektioner, har den dataansvarlige eller en repræsentant for den dataansvarlige ret til at få udleveret dokumentation, herunder logs, stille spørgsmål m.v. med henblik på at konstatere, at databehandleren overholder de krav, der følger af disse Bestemmelser.
- I tilfælde af at Datatilsynet ønsker at foretage en inspektion af de ovennævnte foranstaltninger i henhold til denne aftale, forpligter databehandleren og databehandlerens underdatabehandlere sig til uden yderligere omkostninger for den dataansvarlige at stille tid og ressourcer til rådighed herfor.

Aktindsigt

- Ved udvikling forpligter Databehandler sig til at sikre, at it-løsningen/leverancen tager højde for at der skal kunne gives aktindsigt.
- Ved idriftsætning og under drift er Databehandler forsat forpligtet til at sikre, at løsningen tager højde for at der skal kunne gives aktindsigt.

  Begge dele er lovfæstet i principperne i Offentlighedslovens § 1, stk. 3, samt §§ 11 og 12.
  Sammenholdt med Folketingets Ombudsmandskrav om at, der tages højde for forvaltningsretlige krav i forhold til nye it-løsninger, jf. ombudsmandens notat "Generelle forvaltningsretlige krav til offentlige IT-systemer" som forefindes på https://www.ombudsmanden.dk/myndighedsguiden/specifikke_sagsomraader/generelle_forvaltningsretlige_krav_til_offentlige_it-systemer/
  Såfremt it-løsningen/leverancen ikke tager højde for forvaltningsretlige krav, kan Dataansvarlig opsige Aftalen uden varsel.