Databehandleraftale

Denne aftale er struktureret efter Datatilsynets standardskabelon for databehandleraftaler (standardkontraktsbestemmelser, jf. databeskyttelsesforordningens artikel 28, stk. 3) og er klar til underskrift.

Sådan udfylder I aftalen

1. Udfyld parternes navne, adresser og CVR-numre i afsnit 1. Felter, der skal udfyldes, står i kantede parenteser.
2. For folkeskoler er det som udgangspunkt **kommunen**, der er dataansvarlig. Indsæt da kommunen som "den dataansvarlige" og skolen som kontakt/bruger. Frie grundskoler og efterskoler er selv dataansvarlige.
3. Skriv dato og underskriv begge steder til sidst. Aftalen er et bilag til licensaftalen og træder i kraft ved begge parters underskrift.
4. Bilag A (oplysninger om behandlingen) og bilag B (godkendte underdatabehandlere) er en del af aftalen og skal ikke udfyldes.

---

1. Parterne

Den dataansvarlige:

[Skolens navn]

[Adresse]

CVR: ***[skolens/kommunens CVR-nr.]***

Kontaktperson: ***[navn, e-mail]***

(herefter "skolen")

Databehandleren:

Økonomispillet v/ August Gammeltoft og Villum Halberg

[postadresse]

CVR: ***[CVR-nr.]***

Kontakt: vshalberg01@gmail.com

(herefter "Økonomispillet")

Parterne har indgået denne databehandleraftale (herefter "aftalen") i forbindelse med skolens licens til undervisningsspillet **Økonomispillet** (også kendt som *Livsvejen*). Aftalen er et bilag til licensaftalen og gælder så længe Økonomispillet behandler personoplysninger på skolens vegne.

2. Baggrund og formål

Skolen er dataansvarlig for de personoplysninger, der behandles, når skolens elever og lærere bruger Økonomispillet i undervisningen. Økonomispillet behandler alene oplysningerne på skolens vegne og efter skolens dokumenterede instruks, som er beskrevet i denne aftale med bilag.

Behandlingens formål er udelukkende at **levere spillets funktionalitet i klasserummet**:

- at eleverne kan deltage i et fælles klasserum (multiplayer) via en klassekode,
- at spillets fremdrift gemmes, så en elev kan fortsætte efter genindlæsning eller i en senere lektion,

- at læreren kan følge klassens fremdrift live i læreroverblikket (elevens brugernavn, alder i spillet, formue i spillet, livspoint m.v.),
- at eleven kan logge ind i sit klasserum igen med brugernavn og adgangskode (og at læreren kan hjælpe en elev, der har glemt sin adgangskode).

Derudover indsamler spillet **anonym, aggregeret statistik** til forbedring af spillet (fx hvor mange elever der svarer rigtigt på et bestemt spørgsmål). Denne statistik er designet, så den **ikke indeholder personoplysninger** (se afsnit 6.2 og bilag A), og falder derfor som udgangspunkt uden for aftalens anvendelsesområde. Den beskrives alligevel her for fuld gennemsigtighed.

3. Behandlingens karakter og omfang

Se **bilag A** for en udtømmende beskrivelse af:

- kategorier af registrerede,
- typer af personoplysninger,
- behandlingens karakter, formål og varighed.

Kort sagt: Spillet behandler **elevens selvvalgte brugernavn, en hash af den selvvalgte adgangskode og spildata** (fiktive økonomiske valg i spillet). Adgangskoden kan ikke læses af læreren, kun nulstilles (se punkt 6.1). Der behandles **ingen følsomme personoplysninger**, ingen CPR-numre, ingen e-mailadresser, ingen karakterer og ingen oplysninger om elevens virkelige økonomi eller familie.

4. Databehandleren handler efter instruks

1. Økonomispillet behandler kun personoplysninger efter dokumenteret instruks fra skolen, medmindre behandling kræves i henhold til EU-ret eller dansk ret.
2. Skolens instruks er ved aftalens indgåelse: *Behandl elev- og lærerdata i det omfang, det er nødvendigt for at levere spillets funktioner som beskrevet i bilag A — og intet andet.*
3. Økonomispillet underretter omgående skolen, hvis en instruks efter Økonomispillets mening er i strid med databeskyttelsesforordningen eller anden databeskyttelseslovgivning.
4. Økonomispillet må ikke bruge de oplysninger, der behandles for skolen (brugernavn, adgangskode-hash og spil-state i klasserum og gemte spil), til egne formål, herunder markedsføring, profilering eller salg til tredjeparter.
5. **Statistik, der er adskilt fra klasserumsdata.** Spillet sender samtidig læringsstatistik fra elevens browser direkte til Økonomispillets statistik-database. Den læser ikke fra og kobles aldrig til klasserumsdata. Statistikken indeholder hverken navn, brugernavn, adgangskode, e-mail eller IP-adresse, men en tilfældig sessions-id og en hash af klassekoden. Den er derfor *pseudonymiseret* og behandles forsigtigt som personoplysninger (rå events slettes efter højst 12 måneder; tal vises kun for mindst 5 personer).

- Økonomispillet fastlægger selv formål og midler for statistikken og er derfor **selvstændigt dataansvarlig** for den, jf. bilag A.6. Det er ikke en behandling, Økonomispillet udfører på skolens instruks.
- Formål: at forbedre og kvalitetssikre spillet, dokumentere læringsgevinst og drive tjenesten. Retsgrundlag: databeskyttelsesforordningens art. 6, stk. 1, litra f (legitim interesse). Økonomispillet må ikke bruge statistikken til andet, ikke sælge den og ikke samkøre den med klasserumsdata eller navne.
- Skolen oplyses herved om statistikken. Skolen kan til enhver tid gøre indsigelse (art. 21) eller kræve, at klassens bidrag fjernes. Økonomispillet sletter da alle events og aggregerede tal for klassekodens hash inden for 14 dage (afsnit 11).

5. Fortrolighed

1. Kun personer, der er autoriseret af Økonomispillet, og som har et konkret behov, har adgang til personoplysningerne. Ved aftalens indgåelse er det alene August Gammeltoft og Villum Halberg *(+ evt.*

medudviklere — angives konkret).

2. Autoriserede personer er underlagt fortrolighedsforpligtelse.
3. Adgangen gennemgås løbende og inddrages, når den ikke længere er nødvendig.

6. Behandlingssikkerhed — faktiske tekniske og organisatoriske foranstaltninger

Foranstaltningerne nedenfor beskriver den **faktiske arkitektur** i Økonomispillet (jf. spillets `PRIVACY.md` og databasens Security Rules i `database.rules.json`) — ikke generiske hensigtserklæringer.

6.1 Dataminimering ved design

- Når en elev joiner et klasserum, vælger eleven et **brugernavn og en adgangskode** (begge påkrævet). Der oprettes ingen e-mail-konto, og ingen oplysninger om elevens virkelige identitet indsamles. Eleven opfordres til at bruge et kaldenavn og **ikke** en adgangskode, som bruges andre steder.
- **Adgangskoden gemmes som hash** (SHA-256 af klassekode, brugernavn og adgangskode) på `rooms/<kode>/players/<id>/pwHash`, ikke i klartekst. Hverken Økonomispillet eller læreren kan læse den; læreren kan nulstille den ("Nulstil" i læreroverblikket) og får da en ny kode, der kun vises i det øjeblik. Formålet er at forhindre utilsigtet overtagelse af en kammerats spil. Den sendes aldrig til den anonyme statistik og gemmes ikke i skyen sammen med det gemte spil. Ældre klartekst-poster omskrives automatisk til hash.
- Der indsamles **ikke** e-mail, CPR, fødselsdato, klassetrin, karakterer, geolokation eller enhedsprofiler, og spillet sætter ingen tredjepartscookies eller -trackere (ingen Google Analytics, Meta Pixel el.lign.). Spillet henter hverken fonts, scripts eller andet indhold fra eksterne servere; alt leveres sammen med spillet.
- "Alder" og "formue" i spillet er **fiktive spilværdier** — ikke oplysninger om eleven selv.
- Spillet kan afvikles i **solo-tilstand**, hvor intet navn og ingen spildata overhovedet sendes til en server (kun anonym statistik, se 6.2).

6.2 Adskilte datazoner med teknisk håndhævelse

Databasen er opdelt i adskilte zoner med hver sine adgangsregler:

- **Klasserumsdata** (`rooms/`, `saves/`): elevens brugernavn, adgangskode og spil-state, knyttet til en tilfældigt genereret klassekode på 4 bogstaver. Data er midlertidige og slettes efter forløbet (se afsnit 11). **Kendt begrænsning:** databasen kræver ikke et egentligt login for at læse disse noder. Beskyttelsen består i, at klassekoden er tilfældig, at hverken skolens eller klassens navn indgår i dataene, og at skolens elever kun får klassekoden af læreren. Økonomispillet arbejder på at stramme adgangsreglerne (autentificering pr. rum). Skolen skal indtil da vurdere risikoen i sin egen risikovurdering og opfordre eleverne til at bruge kaldenavne og en adgangskode, de ikke bruger andre steder.
- **Anonym statistik** (`analytics/`): databasens Security Rules **afviser på serverniveau** enhver skrivning, der indeholder felterne `name`, `playerName`, `classCode`, `email`, `ip` eller `userId`. Rå events er append-only (kan skrives, men ikke læses eller ændres fra klienten). Klassekoden hashes (SHA-256 med pepper, forkortet til 16 hex-tegn), før den sendes, så samme klasse kan aggregeres uden at koden er læselig. Da koden er kort og peberet ligger i spillets kode, er hashen en pseudonymisering, ikke en uigenkaldelig anonymisering. Rå events slettes derfor efter højst 12 måneder, og statistikken behandles forsigtigt, som om den kunne være personoplysninger. Aggregerede tal vises aldrig for grupper under 5 personer (k-anonymitet).
- De to zoner **kobles aldrig sammen**: Læreroverblikket læser kun klasserumsdata; statistik-dashboardet læser kun aggregerede, anonyme tal.

6.3 Infrastruktur

- Data lagres i **Firebase Realtime Database, region europe-west1 (Belgien)**. Selve spildataene forlader ikke EU.
- Al trafik mellem browser og database er krypteret (TLS/HTTPS).
- Selve spillet leveres som statiske filer via Netlify (CDN); der lagres ingen spillerdata hos Netlify. Fonts, diagrambibliotek og Firebase-biblioteket leveres sammen med spillet, ikke fra Google, jsDelivr eller andre CDN'er.
- Sletning af klasserumsdata (180 dage) sker via et dagligt serverjob (Netlify scheduled function med servicekonto). Sletning efter anmodning sker manuelt inden for 14 dage.
- Rå statistik-events slettes automatisk efter **maksimalt 12 måneder**.

6.4 Organisatoriske foranstaltninger

- Databasens adgangsregler er versionsstyrede og gennemgås ved enhver ændring af dataindsamlingen.
- Nye indsamlingsfunktioner designes efter princippet om dataminimering; enhver udvidelse, der ville kunne identificere enkeltelever, kræver særskilt aftale med skolen og implementeres i givet fald som eksplicit opt-in.
- Økonomispillet stiller på skolens anmodning en beskrivelse af risikovurderingen af behandlingssikkerheden (art. 32) til rådighed.

7. Underdatabehandlere

1. Skolen giver ved aftalens indgåelse en **generel godkendelse** af, at Økonomispillet anvender underdatabehandlerne i **bilag B**.
2. Økonomispillet underretter skolen skriftligt mindst **30 dage** før tilføjelse eller udskiftning af en underdatabehandler. Skolen kan gøre begrundet indsigelse; kan parterne ikke nå til enighed, kan skolen opsige licensen til udløb af den betalte periode.
3. Økonomispillet pålægger underdatabehandlere de samme databeskyttelses- forpligtelser som i denne aftale (via underdatabehandlerens databehandlervilkår, fx Google Cloud Data Processing Addendum).

8. Overførsel til tredjelande

- Spillerdata (klasserumsdata) lagres i EU (Belgien). Google er en amerikansk koncern, og Google Cloud kan i begrænset omfang have adgang fra tredjelande til support og drift; overførslen er dækket af Googles databehandlervilkår med EU-Kommissionens standardkontraktbestemmelser og EU-U.S. Data Privacy Framework. Når en elevs browser forbinder til databasen, modtager Google teknisk set elevens IP-adresse. Økonomispillet gemmer eller bruger den ikke.
- Netlify, Inc. er etableret i USA. Netlify leverer alene spillets statiske filer og behandler i den forbindelse forbindelsesdata (herunder IP-adresser) transient. Overførselsgrundlag: EU-Kommissionens standardkontraktbestemmelser (SCC) suppleret med EU-U.S. Data Privacy Framework, som Netlify, Inc. er tilmeldt.

9. Bistand til den dataansvarlige

1. Økonomispillet bistår skolen med at besvare anmodninger fra registrerede (indsigt, berigtigelse, sletning m.v.), i det omfang skolen ikke selv kan håndtere dem. Fordi klasserumsdata er nøglet på klassekode + kaldenavn, kan Økonomispillet finde og slette en konkret elevs eller en hel klasses data på skolens anmodning — normalt inden for **14 dage**.
2. Økonomispillet bistår skolen med oplysninger til brug for konsekvensanalyser (art. 35) og forudgående høringer (art. 36), i det omfang det er relevant for behandlingen.
3. Bistanden er inkluderet i licensen i rimeligt omfang.

10. Underretning om brud på persondatasikkerheden

1. Økonomispillet underretter skolen **uden unødig forsinkelse og senest 48 timer** efter at være blevet bekendt med et brud på persondatasikkerheden, der vedrører oplysninger behandlet for skolen.
2. Underretningen indeholder den information, skolen skal bruge til sin eventuelle anmeldelse til Datatilsynet (bruddets karakter, berørte kategorier og omtrentligt antal, sandsynlige konsekvenser, trufne foranstaltninger).
3. Det er skolen, der som dataansvarlig vurderer, om bruddet skal anmeldes til Datatilsynet og/eller de registrerede.

11. Sletning og returnering af oplysninger

- **Klasserumsdata** (`rooms/` og `saves/`: kaldenavne og spil-state) slettes automatisk **180 dage (ca. et halvt år) efter klassens seneste aktivitet** i spillet — en klasse der spiller hele skoleåret rammes derfor ikke midt i forløbet. Skolen kan til enhver tid anmode om tidligere sletning af en klassekode; sletning sker da inden for 14 dage.
- **Rå statistik-events** slettes automatisk efter maksimalt 12 måneder.
- **Aggregerede, anonyme totaler** (fx "68 % svarede rigtigt på spørgsmål X") indeholder ingen personoplysninger og opbevares uden tidsbegrænsning.
- Ved licensens ophør sletter Økonomispillet alle personoplysninger behandlet for skolen senest 3 måneder efter ophør, medmindre skolen forinden anmoder om udlevering (CSV-eksport er tilgængelig fra læreroverblikket, mens rummet er aktivt). Print og eksport af nulstillede koder er skolens ansvar og skal slettes/makuleres af skolen, når de ikke længere skal bruges.

12. Revision og tilsyn

1. Økonomispillet stiller på anmodning alle oplysninger til rådighed, der er nødvendige for at påvise overholdelse af artikel 28 og denne aftale, herunder: den aktuelle version af databasens adgangsregler (`database.rules.json`), privatlivspolitikken og en beskrivelse af dataflowet.
2. Skolen (eller en revisor bemyndiget af skolen) kan én gang årligt — med rimeligt varsel og uden at forstyrre driften — gennemføre tilsyn med behandlingen. Henset til behandlingens meget begrænsede omfang og karakter gennemføres tilsyn som udgangspunkt skriftligt (dokumentgennemgang).
3. For underdatabehandlerne henvises til deres uafhængige revisionserklæringer og certificeringer (Google Cloud: bl.a. ISO 27001, SOC 2/3).

13. Ikrafttræden, varighed og ophør

- Aftalen træder i kraft ved begge parters underskrift og gælder, så længe Økonomispillet behandler personoplysninger på skolens vegne.
- Aftalen kan ikke opsiges separat, så længe licensaftalen løber.
- Bestemmelserne om fortrolighed og sletning gælder også efter ophør, indtil alle oplysninger er slettet.

Bilag A — Oplysninger om behandlingen

A.1 Formål

Levering af undervisningsspillet Økonomispillet til brug i skolens undervisning: klasserums-multiplayer, gem/fortsæt-funktion og lærerens live-overblik over klassens fremdrift i spillet.

A.2 Behandlingens karakter

Indsamling (elevens egen indtastning), lagring, visning for elevens egen lærer i den aktive klasse-session, og sletning. Ingen samkøring med andre registre, ingen profilering, ingen automatiske afgørelser.

A.3 Kategorier af registrerede

- **Elever** på skolen, der deltager i undervisning med spillet.
- **Lærere**, der opretter og styrer klasserum.

A.4 Typer af personoplysninger

Registreret	Oplysninger	Bemærkning
Elev	Selvvalgt brugernavn	Eleven kan bruge et kaldenavn; skolen bestemmer praksis
Elev	Hash af selvvalgt adgangskode (kan ikke læses; lærer kan nulstille)	Bør ikke være en kode eleven bruger andre steder
Elev	Spildata: fiktiv alder, formue, livspoint, valg og svar **i spillet**	Fiktive spilværdier — siger intet om elevens virkelige forhold
Elev	Tilknytning til klassekode (tilfældig 4-bogstavskode)	Koden indeholder ikke skolens eller klassens navn
Lærer	Evt. navn ved oprettelse af rum; egne noter om elever i læreroverblikket	Noterne lever kun i den aktive session

Der behandles ingen følsomme oplysninger (art. 9), ingen oplysninger om strafbare forhold, ingen CPR-numre, ingen e-mailadresser, ingen karakterer og ingen adfærds- eller trivselsvurderinger.

A.5 Behandlinger uden for aftalen (Økonomispillet er selv dataansvarlig)

Følgende er ikke omfattet af denne aftale, fordi Økonomispillet er selvstændigt dataansvarlig, jf. spillets privatlivspolitik (`PRIVACY.md`): den anonyme statistik (A.6), den frivillige Danmarks-liste (kaldenavn, skolens navn og spiltal, kun hvis eleven selv slår deling til), frivillig feedback/fejlrapporter og lærerens kontaktformular på hjemmesiden.

A.6 Anonym statistik (pseudonymiseret, ikke direkte identificerende)

Spillet sender anonyme læringsstatistik-events (spørgsmåls-ID, rigtigt/forkert, svartid, dilemma-valg, quiz-score, alders-milepæle i spillet, slutresultat i intervaller) med en tilfældig sessions-ID og en hashet klassekode. Klassekoden er kun gemt som kort hash (pseudonymisering). Økonomispillet er selvstændigt dataansvarlig for statistikken (se afsnit 4, punkt 5). Databasens regler afviser teknisk felterne navn, klassekode i klartekst, e-mail, IP og bruger-ID. Tal vises kun aggregeret og kun for grupper på mindst 5.

A.7 Varighed

Behandlingen løber, så længe skolen har licens. Opbevaringsperioder: se aftalens afsnit 11.

Bilag B — Godkendte underdatabehandlere

Underdatabehandler	Ydelse	Lokation for behandling	Grundlag
Google Cloud EMEA Ltd / Google LLC (Firebase Realtime Database)	Database til klasserumsdata og anonym statistik	EU — region europe-west1 (Belgien); begrænset adgang fra tredjelande til support/drift	Google Cloud Data Processing Addendum, SCC + EU-U.S. Data Privacy Framework

Netlify, Inc.	Hosting/CDN af spillets statiske filer (ingen lagring af spillerdata; transient behandling af forbindelsesdata, herunder IP)	USA/globalt CDN	SCC + EU-U.S. Data Privacy Framework

---

Underskrifter

For skolen (dataansvarlig)

Dato: _____
Navn: _____
Underskrift: _____

For Økonomispillet (databehandler) — begge parter underskriver:

Dato: _____	**Dato:** _____
Navn: August Gammeltoft	Navn: Villum Halberg
Underskrift: _____	Underskrift: _____