TEKNISK WHITEPAPER

Aula-Assistent

Dataflow, funktioner og sikkerhedsforanstaltninger

Version 1.2 · 12. november 2026
Udgiver: RexifyIT consulting ApS
Dokumentationsgrundlag: interne kontroller fra 4.–12. november 2026 og den vedlagte funktionsoversigt.

Formål og afgrænsning

Aula-Assistent hjælper forældre og værger med at få overblik over oplysninger fra deres egen Aula-adgang gennem ChatGPT eller Claude. Dokumentet beskriver arkitektur, understøttede læsefunktioner, udvalgte sikkerhedsforanstaltninger og daterede interne kontroller.

Leverandørbeskrivelse. Dokumentet er ikke en uafhængig sikkerhedsaudit, certificering eller juridisk vurdering af GDPR-overholdelse.

Det primære dataflow

AI-assistent → Cloudflare → UpCloud-backend i København → Aula og relevante læringsplatforme. Resultater begrænses og filtreres på backend, før de returneres gennem Cloudflare. De to dataflowfigurer sidst i dokumentet viser produktflow og administrative tjenester særskilt.

Funktionerne ændrer ikke skoleoplysninger i Aula. Autentificering kan dog forny og gemme forbindelsesoplysninger. Den næste side gengiver de ni funktioner fra den leverede funktionsoversigt.

Adgang og forbindelsesoplysninger

Barnespecifikke funktioner kontrollerer, at barnet tilhører den autentificerede forælders adgang. Backend vælger forbindelsesoplysninger ud fra den autentificerede brugerkontekst.

Bruger-ID, Aula-tokens, cookies og forbindelsesmetadata lagres særskilt pr. bruger i krypterede pakker i Google Cloud Firestore. Google Cloud KMS udfører kryptering og dekryptering; UpCloud-backenden bruger de dekrypterede oplysninger under drift.

Aula-forbindelsesoplysninger er ikke det samme som brugerens personlige MitID-PIN eller godkendelseskoder. Kryptering ved lagring betyder ikke, at den backend, der anvender forbindelsen, er afskåret fra oplysningerne.

FUNKTIONSOVERSIGT

Hvilke oplysninger kan Aula-Assistent hente?

Oplysninger hentes fra den tilknyttede forælders eller værges Aula-adgang. Lektier og ugeplaner kan komme fra MinUddannelse eller EasyIQ. Tabellen gengiver den leverede funktionsoversigt; den er ikke i sig selv en test af hver funktion.

Funktion	Beskrivelse
Børn og institutioner `list_children`	Viser de børn, der er tilgængelige gennem din Aula-konto, med navn, institution og en identifikator, der bruges til efterfølgende forespørgsler.
Kalender `get_calendar`	Henter kommende kalenderbegivenheder og skemaoplysninger for ét barn, eksempelvis titel, tidspunkt, lokation og lærer-/vikaroplysninger.
Beskeder `get_messages`	Henter udvalgte, nyere beskeder vedrørende ét barn. Tråde, som Aula markerer som følsomme, fravælges, før beskedindholdet hentes. Ved udtrykkelig anmodning kan ét relevant aktivitetsplanbilag i PDF-format også læses.
Opslag `get_posts`	Henter et begrænset udvalg af opslag fra første side for ét barn. Opslag med en udtrykkelig følsomhedsmarkering fravælges. Ved udtrykkelig anmodning kan ét relevant aktivitetsplanbilag i PDF-format også læses.
Lektier og opgaver `get_homework`	Henter lektier og opgaver for ét barn fra MinUddannelse eller EasyIQ, eksempelvis opgavetitel, fag, afleveringsfrist og færdiggørelsesstatus.
Ugeplaner `get_week_plan`	Henter ugeplaner for ét barn fra MinUddannelse eller EasyIQ, herunder planens tekst og ugeangivelse.
Dagligt overblik `get_daily_overview`	Samler relevante oplysninger for ét barn. Kan også omfatte registrerede komme-/gåoplysninger og afhentningsplaner samt oplysninger fra et aktivitetsplanbilag, når funktionen er aktiveret. Planlagt afhentning holdes adskilt fra faktisk registreret afgang.
Familieoverblik `get_family_overview`	Samler overblik for børnene på din Aula-konto. Kan omfatte de samme oplysningstyper som det daglige overblik samt bilag inden for funktionens begrænsninger.
Dokumenter og bilag `get_documents`	Læser ved anmodning op til tre relevante PDF- eller DOCX-dokumenter fra udvalgte nyere beskeder og opslag for ét barn. Returnerer filtrerede praktiske oplysninger fra eksempelvis invitationer, legegrupper og fremlæggelsesplaner samt status for læsningen. Enkelte navne kan indgå. Funktionen omfatter ikke et komplet historisk arkiv eller tekstgenkendelse fra scannede billeder. Udvælgelsen kræver adgangs- og følsomhedskontrol, understøttet filtype og en kategori genkendt i filnavn eller emne/titel. Se udvælgelsesreglerne på næste side.

Funktionerne ændrer ikke skoleoplysninger i Aula. Filtreringen er ikke en garanti for anonymitet eller for, at alle følsomme oplysninger identificeres. Forbindelses- og sessionsoplysninger behandles særskilt for at etablere og vedligeholde adgangen.

DOKUMENTER OG BILAG · UDVÆLGELSESREGLER

Vi henter ikke alle vedhæftninger

Dokumentlæsning skal være aktiveret, og funktionen skal kaldes for et barn, som den autentificerede forælder har adgang til. Den brede dokumentfunktion er beregnet til forespørgsler om bilag. Der foretages ikke en fuld historisk gennemgang af Aula.

Kontroller før download

Kontrol	Regel
Adgang og kilde	Barnets tilknytning kontrolleres. Bilaget skal komme fra en serverhentet besked eller et opslag inden for den tilladte Aula-kontekst; et vilkårligt fil-ID eller link er ikke nok.
Følsomhedsmarkering	Dokumentudvælgelsen kræver en udtrykkelig ikke-følsom markering for tråde og opslag. Markeringer på den konkrete besked og bilagsmetadata kontrolleres også. Ved hentning revalideres kilde og tilknytning.
Kategori	Filnavn og/eller beskedens emne eller opslagets titel skal matche en understøttet kategori: aktivitets-/uge-/månedsplan, invitation, forældre-/praktisk information, legegruppe eller fremlæggelsesplan (fx »Timen er min«/»præsentationsplan«). Udvælgelsen er regelbaseret, ikke en garanti for dokumentets indhold.
Filtype og adresse	Filer udvælges efter PDF-/DOCX-filendelse; det faktiske format kontrolleres efter hentning. DOC og billedbilag understøttes ikke i denne funktion. Download skal ske via HTTPS fra en af de udtrykkeligt tilladte Aula-værter.
Afgrænset søgning	Der undersøges højst de første 10 tråde i den hentede beskedoversigt, op til 10 beskeder pr. relevant tråd og 20 opslag fra første side. Højst 20 bilagsmetadata pr. kilde og 60 kandidater indgår.
Læsebudget	Højst tre læseforsøg pr. barn og kald; fejl og afvisninger kan bruge budgettet. I familieoverblik læses højst tre pr. barn for de første to børn, altså seks forsøg i alt. Dubletter med samme kilde-URL springes over.
Ressourcegrænser	Download afgrænses til 5 MiB pr. fil. PDF-læsning er begrænset til 30 sider. Der gælder desuden tids-, hukommelses- og tekstgrænser; der returneres højst 24.000 tegn på tværs af dokumenterne.

Kontrol efter download

Teksten undersøges efter hentning. Regler for blandt andet CPR-mønstre, følsomhedsindikatorer, økonomi/betaling og bestemte person-/kontaktlister kan blokere resultatet. Filnavn eller emne med betalingsrelaterede nøgleord kan allerede fravælges før download. Kontrollerne garanterer ikke fuldstændig genkendelse eller anonymitet. Kun accepterede, filtrerede oplysninger returneres.

Sikkerhedsrevalidering kan genhente op til 50 beskeder i en udvalgt tråd eller 50 opslag uden at udvide kandidatgrænserne ovenfor. Automatisk læsning af ét aktivitetsplanbilag i overblik er en særskilt funktion med egne regler.

BEHANDLING OG FILTRERING

Hvad rammer backend?

Backend modtager rå profilsvar og metadata samt relevante kalenderposter, opslag og udvalgte beskedtekster. Lektier og ugeplaner kan hentes fra MinUddannelse eller EasyIQ. Ved aktiverede dokumentfunktioner kan relevante bilag hentes og behandles efter funktionens adgangs- og formatbegrænsninger.

Ved beskeder modtages først trådmetadata. Tråde, som Aula markerer som følsomme, fravælges før hentning af selve beskedteksten. Markeringen er ikke en garanti for indholdet af andre tråde; en almindelig besked kan indeholde følsomme oplysninger.

Privacy-filterets dokumenterede opgaver

- Kontrol af den autentificerede brugers adgang til det valgte barn.
- Fravalg af følsommarkerede beskedtråde før hentning af beskedindhold samt særskilte kontroller ved opslag og bilag.
- Udvælgelse af svarfelter frem for videresendelse af komplette rå Aula-svar.
- Fjernelse af genkendelige e-mailadresser og danske telefonnummermønstre i de tekstfelter, som behandles af tekstfilteret, samt udeladelse af udvalgte tekniske felter.
- Funktionsspecifikke begrænsninger på dokumentformater, antal bilag og de oplysninger, der returneres. Dokumenttekst behandles som kildedata, ikke som instruktioner.

Begrænsninger

> **Filtrering er ikke anonymisering.** Navne og oplysninger om andre personer kan fortsat indgå i resultaterne. Der gives ikke garanti for, at alle følsomme oplysninger identificeres eller fjernes.

Denne version fastslår ikke en generel detektion af helbredsoplysninger i samtlige udgående svar. Kontroller og begrænsninger skal vurderes for den konkrete funktion og release. Historiske tests af en fælles indholdskontrol er derfor adskilt fra beskrivelsen af de dokumenterede funktioner.

Behandling hos AI-modtageren

Returnerede oplysninger kan indgå i brugerens samtale hos ChatGPT eller Claude. Den videre behandling og opbevaring afhænger af AI-tjenesten, kontotypen, aftalen og indstillingerne. Sletning hos RexifyIT sletter ikke automatisk oplysninger i Aula eller hos AI-modtageren.

OPBEVARING, SLETNING OG DRIFT

Aula-indhold og hukommelse

Løsningen er indrettet til at hente skoleindhold efter behov og behandle det som led i den enkelte forespørgsel, frem for at opbygge et indholdsarkiv. Det er ikke i sig selv dokumentation for, at alle datarester fysisk forsvinder, når et svar er sendt.

Driftskontrol 12. november 2026: UpCloud-serveren havde aktiv swap, og backendens hukommelse var delvist flyttet til swap. Det dokumenterer en mulig diskvej, ikke at konkret Aula-indhold blev fundet på disk. Swapindholdet blev ikke læst.

Der er ikke dokumenteret en maksimal levetid for eventuelle datarester i RAM eller swap. UpClouds svar om infrastrukturkopier, hukommelsesdump, snapshots/backups og sletteperioder afventes. Dokumentet lover derfor ikke behandling udelukkende i fysisk RAM.

Tekniske forbindelsesdata og 30-dagesoprydning

Ved releasekontrollen den 9. november blev automatisk oprydning aktiveret med kontrol hvert kvarter. Jobbet håndterer tekniske Aula-forbindelses-, sessions-, OAuth-, installations- og licensposter i aktive datalagre efter dokumenteret abonnementsophør. Fristen er 30 dage efter faktisk ophør; en opsigelse med fremtidig virkning er ikke i sig selv et ophør.

Aktive eller fornyede abonnementer beskyttes mod sletning. Uoverensstemmelser og historiske manuelle licenser uden registreret ophørsdato slettes ikke ud fra gæt. Den første aktive kørsel kontrollerede 73 licenser uden fejl; ingen havde nået slettefristen.

Minimale spærrings- og slettemarkører bevares særskilt for at modvirke genskabelse og kontrollere sletteforløb. De indeholder ikke Aula-indhold eller brugbare tokens/cookies, men kan fortsat være personoplysninger ved sammenkædning. Markørerne har ikke automatisk udløb i den dokumenterede release.

Logs, crash-håndtering og øvrig opbevaring

Den 12. november bestod en syntetisk test af den installerede logredigering, og HTTP-adgangsloggen var deaktiveret. Backend havde roterende lokale driftslogs. Kontrollen var ikke en fuldstændig forensisk gennemgang af alle historiske logværdier.

Containerens core-grænse var nul, men serverens Apport-crashhåndtering var aktiveret. Der blev ikke fundet crashrapporter i de kontrollerede standardmapper; dette er ikke en garanti for, at alle dumpmuligheder er deaktiveret.

30-dagesoprydningen omfatter ikke swapfragmenter, leverandørlogs, backups, supportmails, regnskabsmateriale eller oplysninger hos Aula/AI-tjenester. Disse kategorier skal behandles efter deres egne regler og perioder. Regnskabsmateriale blev ikke ændret ved slettereleasen.

TESTGRUNDLAG OG RÆKKEVIDDE

Daterede interne kontroller

Resultaterne nedenfor vedrører bestemte versioner og tidspunkter. Antal testtilfælde er ikke antal uafhængige angrebsforsøg, og resultater fra forskellige datoer lægges ikke sammen som én sikkerhedsscore.

Dato	Kontrol	Resultat og omfang
4. november	Historiske releasekontroller	Det tidligere whitepaper registrerede 740 relevante tests, herunder 30 tests af den daværende indholdskontrol, samt 17 offentlige adgangskontroller. Dette er historisk evidens og ikke en ny verifikation af alle funktioner i denne version.
9. november	Licens, betaling og sletning	131 kombinerede licens-, betalings-, OAuth- og slettetests, 16 backendtests og 4 integrationstests mod kildekodens entrypoint bestod. Derudover bestod 17 offentlige adgangskontroller.
9. november	Installeret sletteforløb	En syntetisk Firestore-post blev gemt og slettet; forsøg på efterfølgende genskabelse blev afvist. Ældre OAuth-poster blev registreret til oprydning. Aktiv kørsel: 73 licenser kontrolleret, 0 forfaldne sletninger, 0 fejl.
12. november	Aktiv UpCloud-server	Skrivebeskyttet kontrol af swap, containerlagring, crash-håndtering og logmetadata samt syntetisk logtest. Ingen brugercredentials, swapindhold eller rå logtekst blev udlæst.
12. november	Tjenester og dokumentation	Cloud Run-service, administrativt Cloud Run-job og aktiv Cloud Scheduler blev identificeret. Funktionstabellen bygger på den leverede PDF. Dataflowbilaget er revision 2 fra samme dato.

Hvad dokumentationen ikke godtgør

Materialet godtgør ikke, at systemet er uden sårbarheder, at alle følsomme oplysninger identificeres, eller at samtlige juridiske krav er opfyldt. Et komplet brugerforløb gennem alle AI-tjenesters OAuth-login og samtlige dokumentfunktioner er ikke verificeret ved disse kontroller.

Reservebackend og administrative integrationer er vist særskilt. En registreret tjeneste eller en historisk test dokumenterer ikke, at alle dens funktioner er dækket af de samme kontroller. Senere ændringer kan nødvendiggøre ny verifikation.

Dokumentationsgrundlag og kontakt

Grundlaget er det tidligere whitepaper, interne releaseoptegnelser fra 4. og 9. november, den aktive serverkontrol den 12. november, den leverede funktionstabel og de seneste dataflowfigurer. Denne opdatering samler materialet; den udgør ikke en ny samlet sikkerhedsaudit.

Kontakt: hello@rexify.dk · RexifyIT consulting ApS

Login, Aula-indhold og forbindelsesdata

Primært produktflow • Pilene viser behandling og transport, ikke et fælles juridisk ansvar.

FORÆLDER

Browser / app

Starter tilknytning.
Godkender i MitID.

CLOUDFLARE

KV + Durable Objects

OAuth-, aktiverings-, licens- og installationsposter.

Forbindelsen etableres af forælderen.

Bruger-ID og Aula-session er forskellige fra personlige MitID-koder.

LOGININFRASTRUKTUR

MitID / NemLog-in

Unilogin og broker indgår i Aulas loginflow.

Tilknytning

Adgangsstatus

Loginflow

BRUGERENS AI-TJENESTE

ChatGPT / Claude

Kalder MCP-værktøjer.
Modtager minimerede resultater.
Samtaler behandles efter kontoens egne vilkår og indstillinger.

MCP-kald

Minimeret svar

CLOUDFLARE

Workers / MCP-endpoint

Offentlig HTTPS-indgang og OAuth.
Kontrollerer adgang og licens.
Access + Tunnel beskytter transport til backend.
Worker Secrets: driftsadgang.
DNS/TLS håndterer indgangen.

Beskyttet kald

Minimeret svar

UPCLOUD · KØBENHAVN

Primær Python-backend

Henter rå svar og kontrollerer barnets adgang.
Filtrerer og strukturerer resultater.
Bruger dekrypterede tokens og cookies under drift.

Læsning

Råt svar

DATAKILDE

Aula

Returnerer profil- og børnedata, beskedmetadata og udvalgte beskedtekster, kalender, opslag og relevante bilag.

Krypterede forbindelsesoplysninger

Nøgleoperationer

Læringsdata

GOOGLE CLOUD / FORBINDELSESLAGRING OG ADGANG

GOOGLE CLOUD FIRESTORE

Krypteret lagring

Bruger-ID, Aula-tokens, cookies og forbindelsesmetadata gemmes i krypterede pakker.

GOOGLE CLOUD KMS

Krypteringsnøgle

Udfører kryptering og dekryptering. Backend får dekrypterede oplysninger til brug.

IAM / Workload Identity: giver backendens driftsidentitet adgang til Firestore og KMS.

GOOGLE CLOUD RUN · RESERVE

Alternativ backend

Alternativ til UpCloud.
Ikke del af det primære flow.
Valg styres i Cloudflare.
Ingen automatisk fallback.

TILKNYTTEDE DATAKILDER

MinUddannelse / EasyIQ

Lektier og ugeplaner.

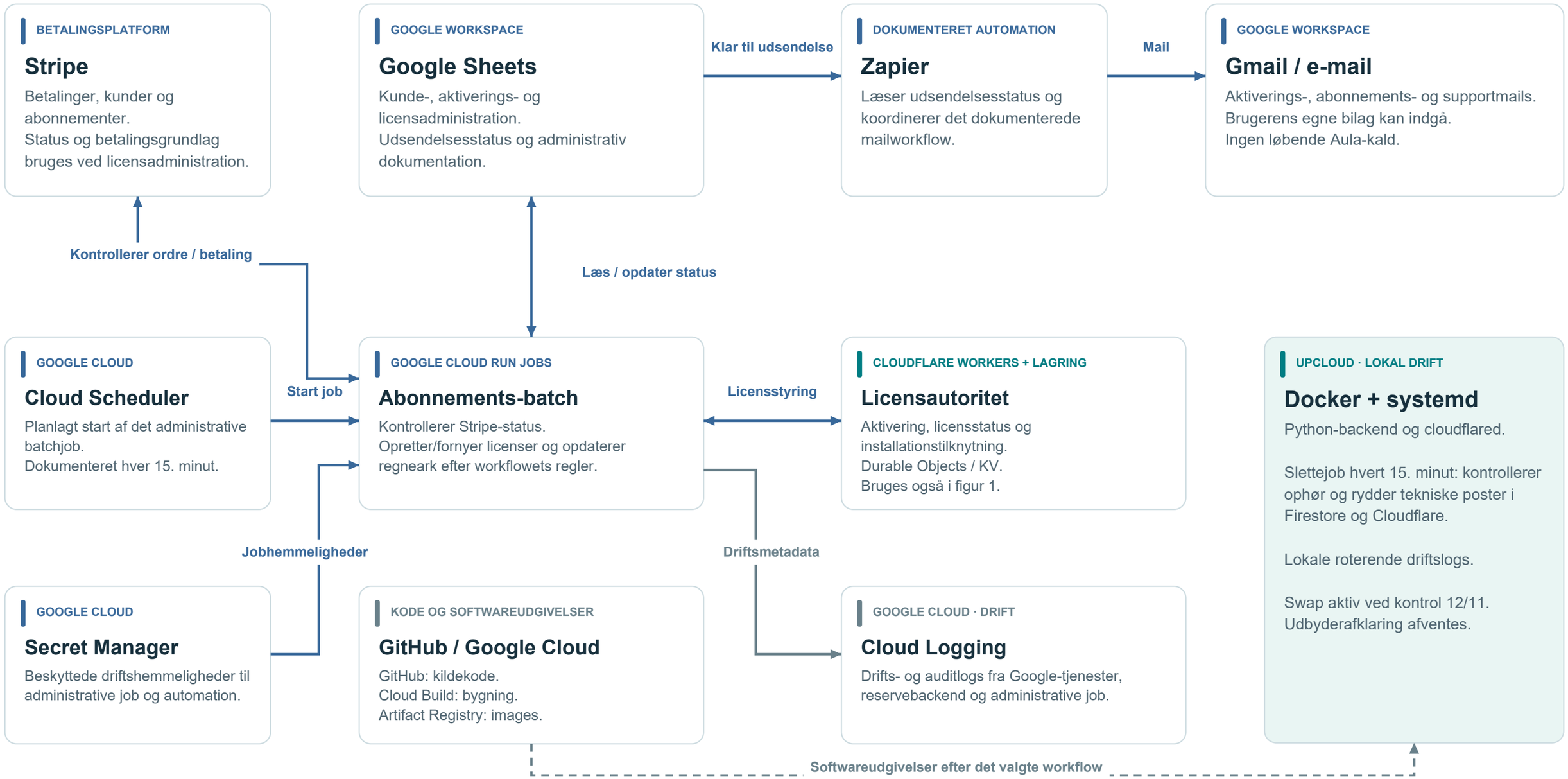
PILE: grøn = indholdsflow · blå = login, forbindelser og administration · stiplet ramme = reserve · grå stiplet pil = softwareudgivelse

Råt Aula-indhold behandles ved den enkelte forespørgsel; følsommarkerede tråde fravælges før hentning af beskedtekst. Filtrering er ikke anonymisering.
Aktiv swap konstateret 12/11: maksimal levetid for datarester er ikke dokumenteret. UpClouds svar om infrastrukturkopier og sletteperioder afventes.

Abonnement, drift og support

Administrationsflow • Disse tjenester er adskilt fra den almindelige hentning af Aula-indhold.

WEBFLOW / aula-assistent.dk: produktinformation, guides, handelsbetingelser, privatliv og henvisning til abonnement.



PILE: grøn = indholdsflow · blå = login, forbindelser og administration · stiplet ramme = reserve · grå stiplet pil = softwareudgivelse

Administrationsdata omfatter bl.a. kontakt-, betalings-, licens- og supportoplysninger. Der er ikke indtegnet et flow af Aula-beskeder til disse tjenester.
Oversigten kombinerer gennemgået kode, driftskontroller og dokumenterede administrative integrationer; den er ikke en fuld verifikation af alle workflows.