APIZ

Compliance-dokument

Juni 2026

Version 1.0

Indhold

1 Sammenfatning

APIZ er en juridisk AI-platform til dansk og EU-ret, drevet af APIZ ApS, Kirsten Walthers Vej 7, 2500 Valby.

Platformen henvender sig til jurister, advokatfirmaer, virksomheder og borgere, der har brug for hurtig og verificerbar adgang til dansk og europæisk lovgivning, retspraksis og forarbejder. APIZ tilbyder tre interfaces, så Kunden kan vælge den integration, der passer bedst:

- APIZ Chatbot – en slutbruger-vendt webgrænseflade med kildebundet AI-assistent.
- APIZ API – et B2B REST-API til programmatisk adgang for legal-tech, advokatfirmaer og forskningsmiljøer.
- APIZ MCP-server – en Model Context Protocol-server, der gør APIZ-data tilgængelig for LLM-klienter.

Platformen er ikke trænet på sit indhold, og kundedata bruges aldrig til at træne eller finjustere AI-modeller. Svar genereres på baggrund af APIZ' underliggende juridiske database (love, bekendtgørelser, domme, EU-ret, forarbejder og høringer). Hvert chatbot-svar viser de kilder, det bygger på, så brugeren selv kan vurdere og verificere AI-output.

Ud over kerne-søgning indeholder APIZ funktionaliteter til upload af dokumenter med AI-assisteret analyse, samlinger til klientsager og søgeagenter med notifikation om nyt indhold på brugerens valgte fagområder.

Dette dokument beskriver APIZ' tilgang til datasikkerhed, privatlivets fred og overholdelse af EU-reglerne. Det skal læses som et supplement til APIZ' til enhver tid gældende vilkår og databehandleraftale.

2 Sikkerhed og privatliv – overblik

APIZ er bygget på følgende grundprincipper for sikkerhed og privatliv. De gælder for alle data, der lagres eller behandles i platformen – uanset om APIZ optræder som dataansvarlig eller databehandler – og er det fundament, som de øvrige afsnit i dette dokument bygger videre på.

Ingen modeltræning
Dine data forbliver private og sikre. APIZ bruger dem aldrig til at træne eller finjustere AI-modeller. Hverken brugerinput, AI-output eller uploadede dokumenter indgår i træningsdata for de underliggende sprogmodeller.

GDPR
Platformen er bygget med GDPR-compliance som grundprincip, så dine data altid behandles med højeste prioritet for sikkerhed og fortrolighed. Databehandlingen er reguleret af en databehandleraftale baseret på Datatilsynets standardkontraktbestemmelser.

EU/EØS infrastruktur
Kundedata lagres og behandles udelukkende inden for EU/EØS hos Microsoft Azure og Google

Cloud Platform. Der sker ingen overførsel af kundedata til tredjelande uden eksplicit retsgrundlag.

Multi-faktor godkendelse (MFA)
APIZ understøtter MFA via Microsoft Entra ID, så identiteten bekræftes med et ekstra sikkerhedslag. MFA kan aktiveres for både slutbrugerkonti og administrative konti.

Single Sign-On (SSO)
Integrér APIZ med eksisterende identitetsløsninger (Microsoft Entra ID / Azure AD) for en sikker og enkel login-oplevelse. Brugeradministration sker via Kundens egen identitetsløsning, og ændringer træder i kraft med det samme.

Kryptering
Al kommunikation mellem klient og server samt mellem servere er krypteret, så netværkstrafikken ikke kan opfanges af tredjeparter. Brugerinput, AI-output og uploadede dokumenter er krypteret in transit og at rest.

Logisk dataisolering
Hver organisations data er logisk isoleret på databaseniveau via strenge adgangskontrolpolitikker, der filtrerer data per bruger og per kunde. En bruger kan aldrig se en anden organisations data.

Rollebaseret adgangskontrol
Medlemmer af en organisation i APIZ kan begrænses til den viden, de har brug for – og intet mere. Privilegeret adgang til produktionsmiljø kræver multi-faktor godkendelse.

Sårbarhedsovervågning
APIZ overvåger løbende kode og infrastruktur for sårbarheder og foretager patch-styring, så identificerede svagheder lukkes hurtigt og kontrolleret.

3 Hvordan vi behandler data

3.1 Dataansvarlig og databehandlers ansvar

APIZ fungerer som dataansvarlig for personoplysninger, der indsamles i forbindelse med levering og administration af de licenserede produkter – herunder aktiviteter såsom kontoadministration, fakturering, kundesupport og analyser relateret til generel produktanvendelse (fx søgninger og logs over interaktioner med tjenesten).

Som dataansvarlig fastlægger APIZ formålet med og midlerne til behandling af brugsdata, som kan analyseres med henblik på produktforbedring, sikkerhedsovervågning, compliance og statistiske formål – altid i overensstemmelse med gældende lovgivning om databeskyttelse.

For alle data, brugeren indtaster i APIZ (input, samtaler, uploadede dokumenter), er Kunden dataansvarlig. APIZ behandler udelukkende disse data på vegne af Kunden og fungerer som

databehandler jf. GDPR. Databehandlingen er reguleret af en databehandleraftale baseret på Datatilsynets standardkontraktbestemmelser, som er en integreret del af kundeaftalen. Det er Kundens ansvar at sikre, at der er et gyldigt retsgrundlag for behandlingen af data i APIZ, og at al behandling overholder gældende lovgivning.

For yderligere information henvises til APIZ' vilkår og databehandleraftale på https://www.apiz.dk/vilkaar og https://www.apiz.dk/databehandling.

3.2 Hvilke data indsamles og lagres

APIZ indsamler og gemmer begrænsede data for at understøtte brugerens arbejde og leveringen af tjenesten.

- Når APIZ optræder som selvstændig dataansvarlig (fx brugeradgang, kundesupport), gemmer APIZ bruger-id og adgangslogdata i relation til APIZ.
- Når APIZ optræder som databehandler i relation til de behandlingsaktiviteter, brugeren udfører i platformen, gemmes både samtaleinput og det uploadede indhold. Typen og arten af uploadet indhold bestemmes udelukkende af Kunden, som er dataansvarlig. Al sådan behandling udføres i overensstemmelse med Kundens instrukser som defineret i databehandleraftalen.

Oplysninger, der indtastes i chatten, bruges udelukkende til at generere et svar til brugeren. De tilgås eller behandles ikke til andre formål, medmindre brugeren vælger at give feedback på et givet svar. I sådanne tilfælde kan de relevante data tilgås af APIZ udelukkende med det formål at forbedre platformen, og disse data anonymiseres og adskilles fra bruger-id'et, før de bruges til udvikling eller kvalitetsforbedring.

3.3 Hvor opbevares data

APIZ er en cloud-baseret SaaS-løsning og opbevarer ikke data på egne lokationer. APIZ anvender Microsoft Azure og Google Cloud Platform til hosting og AI-behandling, i datacentre inden for EU/EØS. Alle data lagres og behandles udelukkende inden for EU/EØS.

3.4 Hvem har adgang til data

Adgang til APIZ' udviklings- og driftsmiljøer er begrænset til autoriseret personale. Tekniske medarbejdere, der er ansvarlige for support og vedligeholdelse af APIZ, kan få adgang til data, hvis det er nødvendigt for at undersøge fejl og ydeevneproblemer. Anonymiserede data anvendes ved optimering af APIZ' svar og ydeevne.

Adgang er rollebaseret, og medlemmer af en organisation kan begrænses til den viden, de har brug for. Privilegeret adgang til produktionsmiljø kræver multi-faktor godkendelse, og alle privilegerede sessioner logges og kan revideres.

3.5 Hvad bruges data til

Data i APIZ, herunder brugerinput, bruges udelukkende til at generere et svar til brugeren. Et uploadet dokument behandles fx udelukkende med henblik på at udføre den valgte analyse (fx

kontraktgennemgang eller compliance-gennemgang), og resultater og udtrukne data bruges udelukkende i forbindelse med den pågældende samtale.

Hverken brugerinput, AI-output eller uploadede dokumenter bruges til at træne AI-modeller.

3.6 Opbevaring og sletning

For at give brugerne mulighed for at vende tilbage til en tidligere interaktion og fortsætte deres arbejde gemmes samtaler for den enkelte bruger. Opbevaringstiderne afspejler en balance mellem brugerens behov for kontinuitet og princippet om dataminimering:

- Ikke-fastgjorte samtaler: tilgængelige i 90 dage efter seneste aktivitet, derefter automatisk slettet.
- Fastgjorte samtaler: opbevares, indtil brugeren sletter dem eller kundeaftalen ophører.
- Uploadede dokumenter: 365 dage fra upload som standard.
- Fakturaer og betalingshistorik: 5 år jf. bogføringsloven.

Brugeren kan til enhver tid slette samtaler og dokumenter manuelt. Handlingen er permanent og irreversibel. Når en samtale slettes, slettes også alle dokumenter, der er uploadet i den.

3.7 Den registreredes rettigheder

Som registreret har man en række rettigheder efter GDPR, herunder retten til indsigt, berigtigelse, sletning, begrænsning, dataportabilitet og indsigelse. Rettighederne kan udøves ved at kontakte APIZ på `APIZ@outlook.dk` eller skrive til APIZ ApS, Kirsten Walthers Vej 7, 2500 Valby.

Læs mere i vores privatlivspolitik på https://www.apiz.dk/privatlivspolitik.

4 Underdatabehandlere

APIZ benytter tredjepartsleverandører til at levere hosting, infrastruktur og AI-behandling, der er nødvendige for driften af platformen. Leverandører kategoriseres efter den sikkerhedsrisiko, deres tjenester udgør, og alle leverandører med middel og høj risiko skal udfylde et spørgeskema om informationssikkerhed og bestå en sikkerhedsvurdering.

Når APIZ optræder som databehandler på vegne af en kunde, anvendes følgende godkendte underdatabehandlere:

- Microsoft – Microsoft Azure Cloud Platform og tjenester, hostet i datacentre inden for EU/EØS.
- Google – Google Cloud Platform og tjenester, hostet i datacentre inden for EU/EØS.
- Anthropic – Claude AI-modeller via EU-hosted endpoints.
- Mistral AI – OCR og embedding-tjenester, EU/EØS.

APIZ bruger Azure OpenAI (via Microsoft Azure), Google Vertex AI (via Google Cloud Platform), Anthropic Claude og Mistral AI til AI-drevet behandling for at generere svar baseret på APIZ' juridiske indhold og brugerinput.

> Vi forbeholder os ret til at ændre eller opdatere de specifikke store sprogmodeller (LLM'er), der anvendes, forudsat at enhver udskiftning er inden for disse udbyderes nuværende serviceudbud og hostes under samme EU/EØS-dataplaceringskontroller.

Brugen af disse underdatabehandlere, deres roller, hostingplaceringer og gældende sikkerhedsforanstaltninger er dokumenteret i databehandleraftalen mellem APIZ og kunden. Aftalen definerer det nøjagtige omfang af behandlingen, databeskyttelseskontroller og slettefrister for de data, der håndteres af underbehandlere.

Tilsyn med højrisiko-leverandører gennemgås årligt, og leverandørers sikkerhedshændelser overvåges løbende.

5 AI-etik og -styring

APIZ strukturerer AI-governance omkring de syv etiske principper, der er fastsat i præamblen til EU's AI-Act, gennem en risikobaseret tilgang. Platformen er designet som et hjælpemiddel, der understøtter, men ikke erstatter, menneskelig beslutningstagning.

APIZ er et beslutningsstøtteværktøj under menneskelig kontrol og betragtes ikke som et højrisiko-AI-system efter EU AI Act. AI-Act regulerer primært højrisiko-AI-systemer som defineret i artikel 6 og bilag III, og APIZ falder ikke ind under disse kategorier, da platformen ikke bruges til beslutninger med væsentlig indvirkning på individers grundlæggende rettigheder, sundhed eller sikkerhed.

5.1 Menneskelig kontrol og citation grounding

Brugerne informeres via brugergrænsefladen, login-flow og brugerbetingelserne om, at APIZ kun skal bruges som et hjælpeværktøj og ikke kan erstatte professionel juridisk rådgivning. Hvert chatbot-svar indeholder et tydeligt disclaimer.

APIZ giver brugerne indsigt i hvilke kilder, svaret bygger på (med direkte links og citater), så brugeren selv kan vurdere og verificere AI-output. Hvis platformen ikke har tilstrækkelig evidens til at give et sikkert svar, kommunikeres dette tydeligt, og brugeren opfordres til at verificere selv.

5.2 Teknologisk robusthed og kvalitetssikring

APIZ' tekniske robusthed og sikkerhed sikres gennem et risikostyringsframework i overensstemmelse med EU's AI-Act.

Hver ændring af kodebasen eller de underliggende sprogmodeller evalueres med interne benchmarks og kvalitetstests udført af jurister, før den frigives til produktion. Det juridiske indhold opdateres løbende, og nyt indhold frigives først, når test og kvalitetskontrol er bestået. Platformen gennemgår løbende sikkerhedstests for at opdage og afhjælpe sårbarheder.

5.3 Privatlivets fred og datastyring

APIZ opretholder privatliv og datastyring gennem dataminimering og security-by-design. Kun de data, der er nødvendige for at generere et svar, behandles, og al kommunikation mellem klient og server samt mellem servere krypteres.

Behandlingen af brugsgenererede data er baseret på legitime interesser jf. artikel 6, stk. 1, litra f i GDPR, og de registrerede kan udøve deres rettigheder ved at kontakte `APIZ@outlook.dk`.

5.4 Gennemsigtighed

APIZ er designet til at være gennemsigtig om muligheder, begrænsninger og drift. Brugere informeres tydeligt om, at de interagerer med AI, og hvert svar viser de kilder, det bygger på.

6 Brugeradministration

Adgang til APIZ gives via SSO med Microsoft Entra ID, via personlige brugerkonti udstedt af APIZ, eller via API-nøgler og MCP-credentials til programmatisk adgang. En bruger kan logge ind fra højst tre (3) enheder ad gangen. Kunden og dens brugere må ikke videregive loginoplysninger til tredjeparter.

Single Sign-On (SSO)
APIZ integrerer med Microsoft Entra ID (Azure AD), så Kunden kan administrere brugeradgang via egne identitetsstyringspolitikker. Det muliggør sikkert login med multi-faktor godkendelse, anvendelse af Kundens adgangskodepolitikker og adgangslogning i Kundens egne systemer. Ændringer i brugeradgang træder i kraft med det samme.

Multi-faktor godkendelse
APIZ understøtter MFA via Entra ID, så identiteten bekræftes med et ekstra sikkerhedslag. MFA kan håndhæves for alle brugere eller alene for privilegerede konti efter Kundens valg.

Personlige legitimationsoplysninger genereret af APIZ
Hvis Kunden ikke bruger SSO, kan APIZ udstede personlige logins, som brugeren anvender til at tilgå platformen. Disse legitimationsoplysninger administreres og vedligeholdes af APIZ.

B2B API-nøgler og MCP-credentials
APIZ udsteder API-nøgler og MCP-credentials til programmatisk adgang. Nøglerne gemmes som hashes, og plaintext-værdien udleveres kun ved oprettelse. Adgangen kan til enhver tid tilbagekaldes uden at påvirke øvrige integrationer.

En personlig adgangskode er aktiv indtil kundekontraktens ophør eller medarbejderens ansættelse hos Kunden ophører. Kunden er ansvarlig for at underrette APIZ om enhver ophørt ansættelse, da retten til at bruge den personlige adgangskode ophører straks fra ansættelsens ophørsdato.

7 Tilgængelighed

APIZ er udviklet med fokus på digital tilgængelighed for alle brugere. Løsningen vedligeholdes og udvikles i overensstemmelse med WCAG-standarder, hvilket sikrer, at indhold og funktioner er:

- Opfattelige: Information og brugergrænseflade kan opfattes af alle brugere, fx gennem klar kontrast, alternativ tekst og tekst-til-tale-funktioner.
- Betjenelige: Alle interaktioner og navigation kan udføres via tastatur og skærmlæsere.
- Forståelige: Kommunikation og funktioner er klare og intuitive, så alle brugere kan udnytte platformen fuldt ud.
- Robust: Indholdet kan fortolkes af en lang række enheder og hjælpemidler og understøtter fremtidige standarder.

Tilgængeligheden overvåges løbende, og dokumentation er tilgængelig på anmodning.

8 Brud, ansvar og revision

8.1 Underretning om brud på datasikkerheden

APIZ underretter Kunden uden unødig forsinkelse i tilfælde af et brud på databeskyttelsen, der vedrører Kundens brugere. Underretningen indeholder de oplysninger, der er nødvendige for, at Kunden kan opfylde sine egne forpligtelser efter GDPR, herunder anmeldelse til Datatilsynet inden for 72 timer hvor det er relevant.

8.2 Ansvar

APIZ' licensvilkår angiver udtrykkeligt, at APIZ er et støtteværktøj og ikke erstatter professionel juridisk rådgivning. APIZ kan ikke holdes ansvarlig for juridiske beslutninger, som Kunden træffer på baggrund af AI-output. Brugeren har et selvstændigt ansvar for at vurdere og verificere de kilder, som AI-svar bygger på.

8.3 Revisionslog

Version	Gyldig fra	Beskrivelse
1.0	2026-06-01	Udarbejdelse af APIZ Compliance-Dokument.

9 FAQ

Træner APIZ på mine data?
Nej. Hverken brugerinput, AI-output eller uploadede dokumenter bruges til at træne eller finjustere AI-modeller. APIZ' underliggende sprogmodeller leveres af Microsoft, Google, Anthropic og Mistral, som ikke modtager kundedata til træningsformål.

Hvor hostes mine data?
Udelukkende inden for EU/EØS hos Microsoft Azure og Google Cloud Platform. Der sker ingen overførsel af kundedata til tredjelande uden eksplicit retsgrundlag.

Hvad sker der hvis jeg sletter en samtale?
Hele samtalen – inklusive alle uploadede dokumenter og AI-output – slettes permanent og irreversibelt. Slettede data kan ikke gendannes.

Hvor længe opbevares mine uploadede dokumenter?
365 dage som standard fra upload-dato. Brugeren kan til enhver tid slette tidligere, og handlingen er permanent og irreversibel.

Hvilke AI-leverandører bruger APIZ?
Microsoft (Azure OpenAI), Google (Vertex AI), Anthropic (Claude) og Mistral AI til OCR og embeddings. Alle hostes inden for EU/EØS. Vi forbeholder os ret til at skifte mellem leverandørernes modeller, forudsat at hosting-vilkår er uændrede.

Tilbyder APIZ et API?
Ja. APIZ tilbyder både et B2B REST-API og en MCP-server (Model Context Protocol). Kontakt os for adgang og dokumentation.

I hvilke lande opererer APIZ?
APIZ er lanceret i Danmark. Platformen dækker dansk og EU-ret og henvender sig primært til brugere, der arbejder med dansk og europæisk lovgivning.

Hvordan adskiller APIZ sig fra traditionelle databaser?
APIZ er bygget specifikt til juridisk informationssøgning med AI som integreret del. Platformen kombinerer hybrid søgning (klassisk fuldtekstsøgning og semantisk vektorsøgning) med citation-grounded AI-svar. Hvert svar peger tilbage til den underliggende retskilde, så brugeren selv kan vurdere AI-output.

For spørgsmål kontakt `APIZ@outlook.dk` eller skriv til APIZ ApS, Kirsten Walthers Vej 7, 2500 Valby.