Compliance Whitepaper

- KAILA og KAILA Flow -

Version 5.0
Juni 2026

KARNOV GROUP

Indholdsfortegnelse

1. Indledning

AI-platformen[1] er en AI-assistent, der er udviklet af Karnov Group. AI-platformen er en informations- og workflowløsning designet til juridiske fagpersoner, der har brug for adgang til juridiske kilder og løsninger i deres arbejde. AI-platformen kombinerer indhold fra Karnov Groups Licenserede Produkter – herunder kommenterede love og regler, retspraksis, onlinebibliotek og andet juridisk materiale – for at understøtte juridisk research, analyse og juridiske arbejdsgange.

Brugere kan udnytte de Licenserede Produkter til at søge, analysere, fortolke, organisere og arbejde med juridisk information, der er relevant for deres juridiske forhold og professionelle aktiviteter. Løsningerne kan også hjælpe brugere med at effektivisere juridiske processer, håndtere opgaver, generere arbejdsdokumenter og støtte beslutningstagning inden for juridiske arbejdsgange.

Dette whitepaper beskriver vores forpligtelse til datasikkerhed, privatlivsbeskyttelse og overholdelse af EU-reglerne vedr. AI-platformen. AI-platformen er ikke trænet i Karnov Groups indhold, men baserer sine svar på indholdet. Alle brugere har adgang til chatten og kan stille spørgsmål i applikationen via tekstindtastning og upload af dokumenter.

Dette giver brugeren mulighed for at tilføje præcis kontekst og lade AI-platformen analysere materialet – for eksempel ikke-offentliggjort retspraksis fra kundens arkiver.

2. Privacy

2.1 Dataansvarlig og databehandler ansvar for vores licenserede produkter

Karnov Group fungerer som dataansvarlig for personoplysninger, der indsamles i forbindelse med levering og administration af vores licenserede produkter og vores tjenester – herunder aktiviteter såsom kontoadministration, fakturering, kundesupport og analyser relateret til generel produktanvendelse (f.eks. søgninger og logs over interaktioner med vores tjenester).

Som dataansvarlig fastlægger Karnov Group 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, som brugeren indtaster i AI-platformen (herunder input og uploadede dokumenter), er Kunden dog dataansvarlig. Karnov Group behandler udelukkende disse data på vegne af Kunden og fungerer som databehandler som defineret i GDPR. Databehandlingen i AI-platformen er reguleret af en databehandleraftale (DBA), som er en integreret del af kundeaftalen. Det er

[1] KAILA (jura) + KAILA Flow

kundens ansvar at sikre, at der er et gyldigt retsgrundlag for behandlingen af data i AI-platformen, og at al behandling overholder gældende lovgivning.

For yderligere information henvises til Karnov Groups til enhver tid gældende licensvilkår.

2.2 Data indsamling i AI-platformen

AI-platformen indsamler og gemmer begrænsede data for at understøtte brugerens arbejde og leveringen af tjenesten.

- Når Karnov Group fungerer som selvstændig dataansvarlig (f.eks. brugeradgang, kundesupport osv.), gemmer Karnov Group bruger-id og logs omkring adgang i relation til AI-platformen.
- Når Karnov Group fungerer som databehandler i relation til behandlingsaktiviteter inden for AI-platformen gemmer virksomheden både samtaleinput og alt uploadet indhold. Typen og arten af uploadet indhold bestemmes udelukkende af Kunden, som er Dataansvarlig. AI sådan behandling udføres i overensstemmelse med kundens instrukser som defineret i databehandleraftalen (DBA).

Oplysninger, der indtastes i AI-platformen, 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 – både brugerens input og KAILAs output – tilgås af Karnov Group udelukkende med det formål at forbedre KAILA. Det er vigtigt at bemærke, at disse data altid vil blive anonymiseret og adskilt fra bruger-id'et, før de bruges til udvikling eller kvalitetsforbedring.

2.3 Dataopbevaring i AI-platformen

AI-platformen er en cloudbaseret SaaS-løsning, hvilket betyder, at data ikke opbevares på Karnov Groups egne lokationer. I stedet bruger Karnov Group både Microsoft Azure platform og Google Cloud Platform og som følge heraf behandles alle data udelukkende inden for EU/EØS.

2.4 Adgangskontrol og tilladelser til AI-platformen

Alle medarbejdere med brugerrettigheder i AI-platformen gennemgår en grundig sikkerhedskontrol, inden de får adgang til vores udviklings- og driftsmiljøer. Tekniske medarbejdere, der er ansvarlige for support og vedligeholdelse af AI-platformen, kan få adgang til data, hvis det er nødvendigt for at undersøge fejl og ydeevneproblemer. Vores data analytikere har kun adgang til anonymiserede data for at optimere AI-platformens svar, udvælgelse og ydeevne.

Karnov Group har implementeret klare procedurer og kontroller for rolle- og adgangsstyring. Al privilegeret adgang til platformen kræver multifaktor-autentificering på bruger-, enheds- og netværksniveau.

2.5 Formål og brug af data

Data i AI-platformen, herunder brugerinput, bruges udelukkende til at generere et svar til brugeren. For eksempel behandles et uploadet dokument udelukkende med henblik på at udføre den valgte analyse (f.eks. kontraktgennemgang, compliance-gennemgang), hvilket betyder, at resultater og udtrukne data udelukkende bruges i forbindelse med den pågældende samtale og ikke bruges til at træne modeller.

2.6 Retsgrundlag for behandling af personoplysninger

Karnov Group behandler de data, der genereres ved brug af de licenserede produkter, på grundlag af legitime interesser, jf. artikel 6, stk. 1, litra f), i GDPR. Oplysningerne bruges til at levere vores licenserede produkter, til markedsføring, til at forbedre it-sikkerhed, til kommunikation og til udvikling af de licenserede produkter.

I AI-platformen udføres behandlingen af personoplysninger i samtaler og uploadede dokumenter af Karnov Group som databehandler i overensstemmelse med kundens dokumenterede instruks i databehandleraftalen (DBA) (artikel 28 i GDPR). Kunden, som dataansvarlig, fastlægger retsgrundlaget for behandlingen af personoplysninger i AI-platformen.

2.7 Den registreredes rettigheder

Som registreret har man en række rettigheder, som man kan udøve ved at kontakte os på privacy@karnovgroup.com eller ved at sende os et brev. Læs mere om registreredes rettigheder i vores privatlivspolitik.

2.8 Tredjeparters behandling af personoplysninger

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

Når Karnov Group fungerer som selvstændig dataansvarlig, kan tredjeparter behandle begrænsede personoplysninger, der er nødvendige for at levere platformen og sikre dens sikre drift.

Når Karnov Group fungerer som databehandler på vegne af en kunde, vil visse godkendte

underdatabehandlere gemme og behandle dataene for at levere tjenesten. Disse underdatabehandlere er:

- Google – Google Cloud Platform og tjenester, hostet i datacentre inden for EU/EØS.
- Microsoft – Microsoft Azure Cloud Platform og tjenester, hostet i datacentre inden for EU/EØS

Derudover bruger AI-platformen Azure OpenAI (via Microsoft Azure) og Google Vertex AI (via Google Cloud Platform) til AI-drevet behandling for at generere svar baseret på Karnov Groups 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 de samme EU/EØS-dataplaceringskontroller.

Brugen af disse underdatabehandlere, deres roller, placering af data og gældende sikkerhedsforanstaltninger er dokumenteret i databehandleraftalen (DBA) mellem Karnov Group og kunden. Denne aftale definerer det nøjagtige omfang af behandlingen, databeskyttelseskontroller og slettefrister, der gælder for data, der håndteres af underbehandlere.

Tilsyn med højrisiko-leverandører gennemgås årligt, leverandørers sikkerhedshændelser overvåges løbende, og indvirkningen af enhver hændelse på Karnov Groups information og tjenester vurderes straks.

2.9 Dataminimering

Karnov Group anvender optimerede dataminimeringsteknikker ved at sikre, at kun nødvendige data bruges til at generere svaret til brugeren.

3. Organisatoriske kontroller

3.1 Rammeværk for data governance

Karnov Group har implementeret en governance-struktur, der definerer og fordeler sikkerhedsansvaret på tværs af organisationen. Der er udviklet politikker, som godkendes af ledelsen og regelmæssigt gennemgås for at sikre effektiviteten.

Der er udpeget en Group CISO, og et informationssikkerhedsudvalg overvåger compliance og risikostyring.

Karnov Group opretholder en tre-linjers forsvarsmodel for at administrere cyber- og informationssikkerhed effektivt.

- Første linje: Forretningsenheder og drift (herunder IT-driftssikkerhed og produktudvikling)

- Anden linje: Cybersikkerhed og compliancefunktion
- Tredje linje: Intern revision og risikostyring (Enterprise Risk Management – ERM)

Hver linje har forskellige ansvarsområder, hvilket sikrer, at governance og risikostyring både er integreret i driften og sikres uafhængigt.

3.2 Håndtering af tredjeparter og forsyningskæde

Karnov Group håndterer tredjepartsrisici gennem en helhedsorienteret ramme for vurdering og monitorering. Før en ny leverandør integreres, vurderer vi leverandørens compliance-status, sikkerhedskontroller og driftsmæssige status for at forhindre sårbarheder i forsyningskæden. Godkendte leverandører er bundet af strenge kontraktlige forpligtelser, der garanterer beskyttelse af datasikkerhed, fortrolighed og privatliv. For at opretholde denne høje grad af sikkerhed gennemgås kritiske leverandører årligt, hvor risikoprofiler opdateres gennem evaluering af aktuelle ISO-certifikater, SOC-rapporter og tilhørende dokumentation.

3.3 Regulatorisk monitorering og implementering

Karnov Group har et dedikeret team, der overvåger og implementerer ændringer i lovgivningen og overvåger relevant lovgivning for at sikre streng overholdelse af al relevant lovgivning i vores jurisdiktion.

3.4 Medarbejdertræning og awareness

Security awareness er en central del af Karnov Groups sikkerhedsstrategi. Alt personale skal gennemføre en årlig uddannelse inden for alle relevante compliance-områder, herunder informationssikkerhed, privatliv og kunstig intelligens.

Der gennemføres phishing-simuleringstests flere gange om året, og de erfaringer, der gøres, anvendes til løbende forbedringer. Derudover afholdes der kvartalsvise security awareness kampagner for at adressere nye trusler og fremme best practice.

3.5 Fysisk sikkerhed

Aktive medarbejdere har adgang til Karnov Groups lokaler via et adgangskort. Kontorerne er beskyttet med alarmsystemer, der er forbundet til et alarmselskab, der er tilgængelige 24/7 for at reagere på enhver aktivering ad en alarm.

4. Tekniske kontroller

4.1 Data centers

Karnov Group benyttes cloud-infrastruktur fra Google Cloud Platform og Microsoft Azure Platform) til hosting af de licenserede produkter, der er udviklet af Karnov Group. Den understøttende infrastruktur er fysisk placeret i europæiske datacentre. Fysisk adgang til serverne er begrænset til autoriseret personale fra Google og Microsoft.

4.2 Dataisolering

AI-platformen anvender logisk dataisolering for at sikre, at brugerdata holdes adskilt og ikke kan tilgås af andre brugere. Brugerens samtaler og uploadede dokumenter lagres krypteret i AI-platformens applikation.

4.3 Kryptering af data

For at beskytte kundedata — herunder alle brugerindtastninger, genererede outputs og uploadede dokumenter — anvender Karnov Group krypteringsmetoder, der lever op til branchestandarden, til beskyttelse af både data i hvile og data under overførsel. Konkret anvender Karnov Group 256-bit Advanced Encryption Standard (AES)-kryptering til 'data at rest' og Transport Layer Security (TLS) 1.3 samt TLS 1.2 til at sikre data under overførsel via netværket.

4.4 Håndtering af krypteringsnøgler

Vores multi-cloud-infrastruktur implementerer en omfattende nøgleadministrationsstrategi, der er skræddersyet til datatilstanden og datamobiliteten. For 'data at rest' på tværs af Azure og GCP benytter vi os af centraliseret lagring, streng administrativ styring og robuste Hardware Security Modules (HSM'er) til at beskytte permanente aktiver. Omvendt omgår 'data in transit' permanent lagring fuldstændigt og er afhængige af automatiske, kortvarige sessionsnøgler, der forsvinder i det øjeblik, de ikke længere er nødvendige. Denne dobbelte tilgang garanterer, at vores lagrede infrastruktur forbliver under streng kontrol under en centraliseret 'source of truth', mens data, der bevæger sig på tværs af netværket, beskyttes af dynamiske engangskoder.

4.5 Adgangskontrol og autentificering

Karnov Group opretholder tekniske adgangskontroller og interne politikker for at sikre, at kun autoriseret personale har adgang til følsomme systemer og data. Tilladelser tildeles i henhold til princippet om mindst mulig adgang og forretningsmæssige behov, med regelmæssige gennemgange for at sikre, at passende adgangsniveauer opretholdes.

4.6 Beskyttelse af netværk

Karnov Group opretholder sikkerheden i backend-netværket med flere lag af beskyttelse og forsvar, herunder sikkerhedsgrupper, proxyservere, overvågning og tests af netværkssikkerhed samt systemer til detektering af indtrængen. Adgangen til produktionsmiljøer via det interne netværk er begrænset til udelukkende autoriseret personale.

4.7 Tekniske sårbarheder

Karnov Group udfører regelmæssigt automatiserede og manuelle sikkerhedstest af applikationer og infrastruktur for at identificere og rette potentielle sikkerhedssårbarheder. Der benyttes desuden uafhængige tjenesteudbydere til at udføre årlige eksterne penetrationstests, og de identificerede problemer løses.

4.8 Applikationssikkerhed

Karnov Group har implementeret en administreret og sikker cyklus for udvikling af software. Nye funktioner og væsentlige ændringer bliver gennemgået. Karnov Group anvender kodescanning og analyse af softwaresammensætning til at opdage og afbøde eventuelle sårbarheder i vores applikationer så tidligt som muligt. Der benyttes uafhængige tjenesteudbydere til at udføre årlige penetrationstests.

4.9 Change Management

Ændringer i applikationskoden, vil følge vores change management proces, som er udviklet til at dokumentere ændringer og sikre, at disse er nødvendige, samt forbedre applikationens funktion. Derudover, bliver alle ændringer gennemgået med 'peer-review' inden de bliver implementeret i produktionsmiljøet.

4.10 Sikkerhed og hændelseslogning

Karnov Group logger adgang og handlinger foretaget af vores medarbejdere. Dette omfatter registrering af oplysninger såsom dato, klokkeslæt og IP-adresser. Sikkerhedsrelevante hændelser, der stammer fra vores infrastruktur, herunder hændelser relateret til autentificering og handlinger foretaget af medarbejdere, logges og revideres. Disse logfiler opbevares og beskyttes mod uautoriseret adgang.

4.11 Pålidelighed, sikkerhedskopiering og forretningskontinuitet

Karnov Groups infrastruktur anvender Google Cloud Platform og Microsoft Azure Platform, som

tilbyder modstandsdygtighed over for naturkatastrofer i flere tilgængelighedszoner.

Vores kundeaftaler definerer ikke kontraktuelle krav angående Recovery Time Objective (RTO) og Recovery Point Objective (RPO). Karnov Group har et internt mål for systemgendannelse fastsat med et defineret Recovery Point Objective.

Vi udfører daglige sikkerhedskopier af produktionsdatabaserne. Sikkerhedskopierne opbevares sikkert ved hjælp af tjenesterne Google Cloud Platform og Microsoft Azure Platform. Sikkerhedskopierne krypteres også og er adgangskontrolleret i overensstemmelse med princippet om mindst mulig adgang.

Der er en redundant arkitektur, hvor ressourcerne er fordelt på geografisk spredte datacentre for at understøtte kontinuerlig tilgængelighed

Derudover testes vores forretningskontinuitets- og katastrofeberedskabsplaner.

5. AI-etik og governance

Karnov Group strukturerer AI-governance og kontrol omkring de syv etiske principper, der er fastsat i præamblen til EU's AI-forordning, gennem en model for risikostyring og en risikobaseret tilgang.

AI-platformen er et beslutningsstøtteværktøj under menneskelig kontrol og betragtes ikke som et højrisiko-AI-system i henhold til AI-forordningens nuværende anvendelsesområde.

AI-forordningen er i øjeblikket kun trådt i kraft for forbudte AI-systemer og modeller til generelle formål, som falder uden for anvendelsesområdet for AI-platformen. Desuden regulerer AI-forordningen primært højrisiko-AI-systemer, som defineret i artikel 6 og bilag III, og AI-platformen falder ikke ind under disse kategorier, da det ikke bruges til beslutninger, der har en væsentlig indvirkning på individers grundlæggende rettigheder, sundhed eller sikkerhed.

5.1 Menneskelig handlemulighed og menneskeligt tilsyn

AI-platformen er designet som et hjælpemiddel, der understøtter, men ikke erstatter, menneskelig beslutningstagning. Det er underlagt menneskelig kontrol og tilsyn og træffer ikke automatiserede beslutninger, der har væsentlig indflydelse på enkeltpersoners grundlæggende rettigheder, sundhed eller sikkerhed. Brugerne informeres via brugergrænsefladen og brugerbetingelserne om, at det kun skal bruges som et hjælpeværktøj og ikke kan erstatte professionel juridisk rådgivning.

Karnov Group har udviklet et AI-forklaringsmodul, der giver brugerne indsigt i AI-platformens proces og funktionalitet.

5.2 Teknologisk robusthed og sikkerhed

AI-platformens tekniske robusthed og sikkerhed sikres gennem vores modelrisikostyringsramme, som er i overensstemmelse med EU's AI-forordning.

Hver ændring af kodebasen eller de underliggende store sprogmodeller evalueres ved hjælp af en kombination af automatiserede interne benchmarks og ekspertvurderinger foretaget af domænespecialister for at verificere ydeevnen og mindske fejl.

Platformen gennemgår regelmæssige sikkerhedstests, herunder automatiseret patch-styring, kontinuerlig sikkerhedsscanning og årlige penetrationstests udført af certificerede fagfolk for hurtigt at opdage og afhjælpe sårbarheder.

For at opretholde pålideligheden og aktualiteten af det juridiske indhold opdateres de underliggende juridiske informationskilder ugentligt og frigives først til produktion, når test og kvalitetskontrol er bestået, hvilket hjælper med at forhindre forringelse og utilsigtede effekter svarene.

Samlet styrker disse kontroller modstandsdygtigheden over for misbrug eller ændringer, der kan påvirke ydeevnen, og reducerer risikoen for utilsigtet skade på brugere og tredjeparter.

5.3 Privatlivets fred og data governance

AI-platformen opretholder privatliv og stærk governance gennem dataminimering, security-by-design og tydelig styring af en applikations livscyklus. Kun de data, der er nødvendige for at generere et svar, behandles, og der anvendes krypteringsmetoder, der lever op til branchestandarder for både 'data at rest' og 'data in transit'

Behandlingen af brugsgenererede data er baseret på legitime interesser i henhold til artikel 6, stk. 1, litra f i GDPR, og de registrerede kan udøve deres rettigheder ved at kontakte privacy@karnovgroup.com.

5.4 Gennemsigtighed

AI-platformen er designet til at være gennemsigtig med hensyn til sine muligheder, begrænsninger og drift. Et AI-forklaringsmodul og en ledsagende vejledning giver indsigt i, hvordan svarene genereres, og muliggør informeret brugerovervågning.

5.5 Mangfoldighed, ikke-forskelsbehandling og retfærdighed

AI-platformens rolle som et værktøj til beslutnings under menneskelig overvågning bidrager til at reducere risikoen for diskriminerende automatiserede resultater. Modelkvaliteten vurderes løbende

ved hjælp af automatiserede interne benchmarks, der suppleres med ekspertvurderinger for at identificere problemer og mindske uberettigede fordomme.

Dataminimering og logisk adskillelse af brugerdata reducerer yderligere eksponeringen for unødvendige attributter. Disse foranstaltninger understøtter samlet set en retfærdig og ligeværdig anvendelse i forskellige sagsbehandlingssammenhænge, samtidig med at mennesker bevarer kontrollen over de endelige beslutninger.

5.6 Social og miljømæssig velfærd

AI-platformen er udviklet og drives i overensstemmelse med Karnov Groups ESG-strategi. Karnov Group er forpligtet til at følge koncernens mission om at bane vejen for retfærdighed, der er knyttet til fem af FN's verdensmål, især verdensmål 16, fred, retfærdighed og stærke institutioner.

Vi er forpligtet til at minimere miljøpåvirkningen ved at reducere drivhusgasemissioner og materialebehov i overensstemmelse med gældende miljølovgivning og med løbende forbedringer gennem mål og overvågning.

Vi respekterer og opretholder internationalt anerkendte menneskerettigheder, fremmer et sikkert, inkluderende og sundt arbejdsmiljø og inddrager interessenter og leverandører for at fremme ansvarlig praksis og sikre, at vores værdikæde opretholder tilsvarende ESG-standarder. ESG-governance sikres gennem bestyrelsens tilsyn, etisk adfærd, integration af ESG-risikostyring i vores ERM-proces, gennemsigtig rapportering og ansvarlighedsmekanismer, herunder vores adfærdskodeks og whistleblower-politik.

5.7 Ansvarlighed

Ansvarlighed for AI-platformen er forankret i Karnov Groups politik for AI og dataetik og Karnov Groups AI-instruktion sammen med en model for risikostyring, der er i overensstemmelse med EU's AI-forordning. Klare tekniske og organisatoriske kontroller – herunder centraliseret adgangsstyring, kun intern adgang til systemer, detaljeret login-logning, regelmæssige sikkerhedstests og penetrationstests samt krypteret kommunikation – fastlægger ansvar og revisionsmuligheder på tværs af tjenesten.

Karnov Group forpligter sig til at underrette kunderne uden unødig forsinkelse om ethvert brud på persondatasikkerheden og præciserer i sine licensvilkår, at AI-platformen er et hjælpemiddel og ikke erstatter professionel juridisk rådgivning, hvilket styrker klare roller og ansvarsområder over for brugere og berørte personer.

6. Produktsikkerhed og kompatibilitet

Som en cloudbaseret platform, kan Karnov Groups Licenserede Produkter tilgås sikkert fra enhver webbrowser på både stationære og mobile enheder. På grund af disse forskellige adgangspunkter og karakteren af det Licenserede Produkt har vi indført foranstaltninger, der giver vores kunder mulighed for at sikre at de Licenserede Produkter er kompatible og kan implementeres sikkert. Disse foranstaltninger omfatter:

6.1 Adgangskontrol

AI-platformen tilbyder flere metoder til adgangskontrol, som kan konfigureres af kundens organisation.

- Single-Sign-On (SSO): Med SAML-baseret SSO kan brugerne få adgang til Karnov Groups AI-platform via en identitetsudbyder (IdP) såsom Microsoft EntraID (tidligere Azure AD) og andre. Dette eliminerer behovet for, at brugerne gentagne gange skal indtaste deres legitimationsoplysninger for hver applikation, hvilket sparer dem tid og samtidig reducerer antallet af angrebsflader.

- 2-trins-godkendelse: Med 2-trins-godkendelse fungerer AI-platformen uden krav om SSO og tilføjer et ekstra beskyttelseslag, når brugerne får adgang til AI-platformen. 2-trins-godkendelse gælder for alle brugere, der logger ind med deres e-mail og adgangskode (for organisationer, der ikke har konfigureret SSO). Karnov Group håndhæver 2-trins-godkendelse med en tidsbegrænset kode, der sendes direkte til brugerens e-mail.

- Adgangskodepolitik: Der er fastsat en adgangskodepolitik for brugere, der logger ind med deres e-mailadresse og adgangskode (for organisationer, der ikke har konfigureret SSO), som kræver mindst 12 tegn.

6.2 Tilgængelighed (digital tilgængelighed)

AI-platformen er udviklet med fuld 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, f.eks. 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 forbedringer dokumenteres i Karnov Groups udviklingslog. Dokumentation om tilgængelighed og testresultater er tilgængelige efter anmodning.

6.3 Browserkompatibilitet

AI-platformen understøtter alle større opdaterede browsere (2 år gamle eller nyere) på både stationære og mobile enheder, men de licenserede produkter er ikke specifikt optimeret til mobil brug. For en komplet oversigt over understøttede browsere, besøg vores side om browserkompatibilitet.

Der kræves internetforbindelse for at bruge løsningen.

6.4 AI-dataflow og brug

Karnov Group anvender flere forskellige modeller afhængigt af use-case og udnytter fordelene ved både generativ AI og sprogmodeller. Brugerinput (f.eks. en prompt eller et dokument) konverteres sammen med kontekst fra AI-platformen til proxy-data, inden den videregives til AI-modellen, som derefter sender resultatet tilbage til proxyen som outputdata (f.eks. et svar eller en analyse), inden det returneres direkte til AI-platformen.

Afhængigt af den anvendte AI-funktion (f.eks. research, planlægning, udarbejdelse osv.) hostes AI-modellen af AI-platformudbyderne (Google Vertex AI eller Azure OpenAI). Dette sikrer, at når AI-platformen opretter forbindelse til AI-modeller, foregår forbindelsen via sikkerhedsforanstaltningerne i Google Cloud Platform og Microsoft Azure, dvs. strenge adgangskontrolforanstaltninger, kryptering og hosting i EU, samt at der ikke foretages modeltræning på brugerinput og uploadede dokumenter.

Det er vigtigt at bemærke, at data ikke lagres permanent hos Google Vertex AI eller Microsoft Azure OpenAI; behandlingen hos vores tredjepartsudbydere af AI-platforme er begrænset til det, der er nødvendigt for at levere det specifikke output til brugeren og for at sikre driften af tjenesten. Dette betyder også, at data kun lagres midlertidigt hos udbyderne, dvs. i den periode, det tager at generere et svar; så snart svaret er leveret til brugeren, findes dataene ikke længere hos AI-platformudbyderne.

6.5 Opbevaring og sletning af data

For at give brugerne mulighed for at vende tilbage til en tidligere interaktion og fortsætte deres arbejde gemmes samtaler – herunder alle brugerinput, genererede output og eventuelle uploadede dokumenter – for den enkelte bruger.

For samtaler, der ikke er fastgjort af brugeren, vil hver samtale være tilgængelig for brugeren i 90 dage efter den seneste aktivitet og derefter blive slettet, medmindre brugeren sletter den tidligere.

Fastgjorte samtaler opbevares, indtil de enten slettes aktivt af brugeren eller indtil kundeaftalen ophører. Dette giver brugeren mulighed for at genbesøge tidligere input eller stille yderligere spørgsmål om det samme emne. Når en samtale slettes, slettes alle dokumenter, der er uploadet inden for den pågældende samtale, også.

Hvis en bruger sletter en samtale manuelt, slettes hele samtalen – inklusive alle uploadede dokumenter og alle relaterede output – permanent og irreversibelt.

7. Orientering og ansvar

7.1 Underretning om brud på datasikkerheden

Karnov Group vil underrette kunden i tilfælde af et brud på databeskyttelsen, der vedrører kundens bruger, uden unødig forsinkelse.

7.2 Ansvar og erstatning

Karnov Groups licensvilkår angiver udtrykkeligt, at AI-platformen er et støtteværktøj og ikke erstatter professionel juridisk rådgivning.

8. Revisionslog

Version	**Gyldig fra**	**Revisionskategori Ny/Opdatering/Formulering/Ingen**	**Beskrivelse af vigtigste revisioner**
1.0	01.09.2024	Ny	Udarbejdelse af KAILA Compliance Whitepaper baseret på brugeres spørgsmål.
2.0	10.01.2025	Opdatering	Ny struktur af whitepaperet, så det passer til ISO27001-rammen, og tilføjelse af detaljer til de specifikke emner.
3.0	05.09.2025	Opdatering	Opdatering for at matche ny upload-funktion og dokumentanalysefunktion, herunder ændring af roller vedrørende behandling af personoplysninger
4.0	19.02.2026	Opdatering	Opdateret i relation til at AI-platformen er blevet et produkt, der tilbydes på tværs ad hele Karnov Group samt fjernelse af muligheden for IP-adgangsrettigheder
5.0	08.06.2026	Opdatering	Ny struktur af whitepaper for at tydeliggøre privacy, AI-etik, organisatoriske og tekniske kontroller samt produkt sikkerhed samt kompatibilitet i nye specifikke sektioner